

An aerial, black-and-white photograph of a damaged building. A large, white, circular object, possibly a satellite dish or a large barrel, sits on the roof. The building's structure is heavily damaged, with many holes and missing sections. The surrounding area appears to be a mix of urban and rural landscape.

HOSTILE DRONES: THE HOSTILE USE OF DRONES BY NON-STATE ACTORS AGAINST BRITISH TARGETS

January 2016



REMOTE CONTROL

Examining changes in military engagement



open briefing

A0326651_1-000001

The Remote Control project is a project of the Network for Social Change hosted by Oxford Research Group. The project examines and challenges changes in military engagement, in particular the use of drones, special operations forces (SOF), private military and security companies (PMSCs) and cyber and intelligence activities.

Chris Abbott is the founder and executive director of Open Briefing. He is also an honorary visiting research fellow in the School of Social and International Studies at the University of Bradford and was the deputy director of the Oxford Research Group until 2009.

Matthew Clarke is an associate researcher at Open Briefing. He is also a freelance campaigner and analyst. He has worked in business, politics and the European NGO community.

Steve Hathorn is a senior analyst at Open Briefing. He is an intelligence analyst with nearly 30 years' experience in the British Army, Defence Intelligence Staff, National Criminal Intelligence Service, United Nations, International Criminal Court and the National Crime Agency.

Scott Hickie is a senior analyst at Open Briefing. He is also a senior policy officer for the New South Wales government. He is a former political adviser and lawyer.

Open Briefing is the world's first civil society intelligence agency. Founded in 2011, its mission is to keep those striving to make the world a better place safe and informed. It provides groundbreaking intelligence and security services to aid agencies, human rights groups, peacebuilding organisations and concerned citizens. It does this so that a stronger civil society can promote alternatives to armed conflict, protect human rights and safeguard the environment. Open Briefing is a bold and ambitious nonprofit social enterprise. It is a unique international collaboration of intelligence, military, law enforcement and government professionals working tirelessly behind the scenes to make a difference.
www.openbriefing.org

Published by the Remote Control project, January 2015

Remote Control Project
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)207 549 0298
media@remotecontrolproject.org

<http://remotecontrolproject.org>

Cover image: Pieces of a Hezbollah UAV (Unmanned aerial vehicle) that was taken down by the Israeli Air Force. Wikimedia Commons, Flickr/ Israel Defense Forces

This report is made available under a Creative Commons license. All citations must be credited to The Remote Control Project and Open Briefing.

Executive Summary	1
Introduction	2
Assessment of commercially-available unmanned vehicles	4
Unmanned aerial vehicles	4
Unmanned ground vehicles	6
Unmanned marine vehicles	8
Assessment of known drone use by non-state actors	10
Lone wolf	10
Terrorist organisations	11
Insurgent groups	12
Organised crime groups	12
Corporations	12
Activist groups	13
Drone countermeasures	14
Regulatory countermeasures	15
Passive countermeasures	16
Active countermeasures	17
Conclusions and policy recommendations	19

Ever-more advanced drones capable of carrying sophisticated imaging equipment and significant payloads are readily available to the civilian market. Unmanned aerial vehicles (UAVs) currently present the greatest risk because of their capabilities and widespread availability, but developments in unmanned ground (UGVs) and marine vehicles (UMVs) are opening up new avenues for hostile groups to exploit.

A range of terrorist, insurgent, criminal, corporate and activist threat groups have already demonstrated the ability to use civilian drones for attacks and intelligence gathering. The best defence against the hostile use of drones is to employ a hierarchy of countermeasures encompassing regulatory countermeasures, passive countermeasures and active countermeasures.

Regulatory countermeasures can restrict the capabilities of commercially available drones and limit the ability of hostile groups and individuals to procure and fly drones. Policymakers should pass stricter regulations limiting the capabilities of commercially available drones in the key specifications affecting hostile drone operations, particularly payload capacity. Particular attention should be paid to limiting the attack and ISR capabilities of UAVs and the attack capabilities of surface UMVs. Manufacturers should be required to install firmware that includes the GPS coordinates of no-fly zones around sensitive fixed locations. Finally, civilian operators of drones capable of carrying payloads should be licenced and the serial numbers of purchased drones registered.

Passive countermeasures alert security to the presence of any drone within a no-fly zone or defensive perimeter around a static or mobile target. They limit the ability of hostile groups and individuals to guide a drone onto a mobile target or target of opportunity or take evasive action against any kinetic defences. The British government should support the research and development of commercial multi-sensor systems capable of detecting and tracking drones within a target area. The government should also make funding available to police forces and specialist units for the purchase of early warning systems and other passive drone countermeasures, including radio frequency jammers and GPS jammers. The government should also relax the regulations restricting the use of radio frequency jammers for protection against hostile drone use around defined key sites.

Active countermeasures can be deployed against drones that still represent a threat despite passive systems being employed. However, the active countermeasures currently available for use in non-military settings are limited. The British government should support the research and development of innovative less-lethal anti-drone systems, such as directional radio frequency jammers, lasers and malware, and set out clear guidelines for the police and military use of kinetic weapons against hostile drones as a last line of defence.

However, such countermeasures are not foolproof. Furthermore, there is also the very real chance that, as with drones themselves, countermeasures will be deployed in turn by some threat groups against British police or military drones. The technology of remote-control warfare is impossible to control; the ultimate defence is to address the root drivers of the threat in the first place.

After long and frequently controversial use by the military, unmanned vehicle technology is now being widely employed in numerous civilian settings. There are unmanned vehicles (or drones) for use in the air (UAVs), on land (UGVs) and on or under the sea (UMVs). Drones are used for leisure and to monitor crops, take aerial photographs, track hurricanes, protect wildlife, monitor traffic, deliver parcels, undertake search and rescue operations and monitor disaster zones. As with many preceding technologies, civilian drones are also used for less benign purposes, including snooping and harassment, drug trafficking and smuggling contraband into prisons.

Ongoing large-scale commercial investment has led to civilian drones becoming cheaper, able to operate over longer ranges and capable of carrying ever-larger payloads. The pace of development has accelerated in recent years, with a vast range of models now available to the civilian customer. There are hundreds of models available, ranging in size from that of an AA battery to prototypes capable of carrying a person.

The legislation governing the civilian use of drones is still evolving. It is struggling to keep up with the speed at which innovative uses are being identified and new drones developed. There are growing concerns over the use of drones by private individuals with little knowledge of aviation rules. In July 2015, the US Department of Homeland Security distributed an intelligence assessment to law enforcement agencies warning of the possibility of criminal or terrorist groups using unmanned aerial vehicles.

In February 2015, the House of Lords EU Select Committee called for the mandatory registration of all civilian drones in the United Kingdom. As legislation stands, anyone can buy a drone and immediately operate it without any training or a license, as long as the drone weighs less than 20 kilograms and it is not being used for commercial purposes. While there are minimal regulations specifically governing the use of ground and marine drones, aerial versions must not be flown within 150 metres of any populated area or 50 metres of any other person, vehicle or structure. The operator is also required to keep the drone in sight, within 500 metres and below 400 feet in altitude. While these simple rules will be followed by the majority of leisure users, those with more nefarious motivations will be less inclined to adhere to them. Even if followed, the regulations cannot account for operator error or technical drone failures. The regulations surrounding UGVs and UMVs are less clear, though existing maritime navigation rules and motor vehicle regulations will likely apply and combat vehicles will likely be covered by existing import/export arms control regimes.

This report details the findings of our study into the hostile use of drones by non-state actors against British targets. While the focus is on unmanned aerial vehicles, we have examined the designs and capabilities of over 200 current and upcoming unmanned aerial, ground and marine systems in order to understand the threat these platforms pose to potential targets. The previous hostile use of drones by non-state actors is also examined. A range of terrorist, insurgent, criminal, corporate and activist threat groups using drones for attacks and intelligence gathering are identified. The report outlines specific recommendations on

the strategies available to mitigate the threat of the hostile use of drones by non-state actors in the short to medium term.

There is no doubt that unmanned vehicles are here to stay and will have a considerable impact on society, both beneficial and detrimental. Although there is still a large gap between the capabilities of military and civilian drones, commercially available drones are giving hobbyists, companies and hostile groups access to capabilities previously only available to the military. Law enforcement agencies and policymakers are struggling to respond appropriately to this development. This report is a contribution to countering that threat.

Unmanned aerial vehicles

The civil and commercial market for unmanned aerial vehicles has grown significantly over the last five years. The increasing uptake by the commercial sector is clearly evidenced in the growing numbers of US Federal Aviation Administration (FAA) exemptions for drone operators to fly UAVs in the National Airspace System (NAS),¹ with the exemptions list showing a broad range of UAV technologies, uses and capabilities.² The UK Civil Aviation Authority (CAA) also has a similar licensing regime for operators using UAVs for commercial aerial work and equipped for data acquisition. As of 11 September 2015, the CAA has issued 1,036 current UAV licences, with an estimated 37% of licences for models in the 7-20 kilogram weight class.³ The civil or hobbyist market is also showing significant growth. Some estimates have the global civil and commercial UAV sector valued at €563.7 million (£418 million).⁴

UAVs are commercially available as off-the-shelf Ready to Fly (RTF), Bind and Fly (BNF – with customisable transmitter) and Plug and Fly (PNF – with customisable transmitter, receiver, battery and charger). Users with no prior UAV flying experience can procure RTF models, and more experienced and knowledgeable users can purchase fully-customisable PNF models. Most commercially available models are rotary multicopter UAVs coming in quadcopter (four propellers), hexacopter (six propellers) and octocopter (eight propellers) variants. Fixed-wing UAVs are more frequently used for commercial deployments in agriculture, public safety, emergency response and ISR. Many UAV manufactures sell individual components, enabling customers to build fully-customised drones. This allows users to achieve specific capabilities, such as flight time, payload capacity, programmable flight, maximum speed and weather hardening. Table 1 lists the most popular and readily-available commercial UAVs across three price points (low end, mid level and high end) and provides basic specification information.

Our analysis of the 202 commercially-available drones listed on the product comparison site SpecOut.com reveals that the listed drones have an average flight time of 18 minutes, an average range of 1,400 metres and median price of \$600 (£390).⁵ Our analysis of FAA Section 333 exemptions indicates that in the United States the agricultural and film sector are using UAVs with the largest capacity for heavier payloads, most likely a result of needing to carry larger sensor and imagery equipment. The public safety, emergency response and infrastructure inspection sectors appear to be relying upon UAVs with greater capacity for all-weather conditions.

¹ Section 333 FAA Modernization and Reform Act of 2012 (FMRA).

² https://www.faa.gov/uas/legislative_programs/section_333/333_authorizations/ and <http://auvsilink.org/advocacy/Section333.html>.

³ <https://www.caa.co.uk/docs/1995/SUA%20Operators%2011Sep15.pdf>.

⁴ INEA Consulting (2014), *Global Commercial and Civil UAV Market Guide 2014-2015*.

⁵ <http://drones.specout.com>.

Specifications affecting hostile UAV operations

A number of specifications are critical to the capabilities and uses of aerial drones. Users seeking greater payload capacity, flight time and range will most likely build customised drones from individual components to specification, requiring some basic technical knowledge. The specifications most relevant to UAV operations include:

Payload

Most RTF and BNF UAVs have a limited payload capacity beyond that required for a gimbal, camera and battery. Those with larger capacity payloads are UAVs aimed at carrying a broader range of imagery capture hardware,

such as LiDAR or infrared camera, or other environmental sensors. Despite some high-profile interest, such as Amazon's nascent Prime Air service, logistics and transport companies have not embraced the use of UAVs because many commercially available platforms have insufficient carrying capacity for goods.

Range

Commercially available UAVs are generally limited in range by signal transmission and image relay distance and battery power (flight time). This means a pilot must be within a particular proximity of the UAV and that flights cannot span a significant distance. Flight time due to power constraints can be partially managed by interrupting flights for battery changes.

Table 1. Select list of commercially available UAVs

Model	Weight	Payload	Flight time	Range	Max speed	Camera	Operating conditions	Price
Parrot BeeBop	0.4 kg	0 kg	12 mins	250 m (extendable)	29 mph	Yes (14MP)	Dry conditions only	£700-900 (RTF)
Blade 350 QX2	1 kg	0.2 kg	10 mins	1,000 m	32 mph	Yes	Dry conditions only	£200-300 (RTF)
3DR IRIS+	0.9 kg	0.2 kg	16 mins	800-1,000 m	40 mph	Yes	Dry conditions only	£500-600 (RTF)
DJI Phantom 2 Vision +	1.2 kg	0.2 kg	25 mins	600 m	33 mph	Yes (14MP)	Dry conditions only	£800-1,200
DJI Phantom 3 Professional	1.2 kg	0.3 kg	28 mins	1,900 m	35 mph	Yes (12MP)	Dry conditions only	£1,000-1,200
Walkera Scout X4	1.7 kg	0.5-1.0 kg	25 mins	1,200 m	40-50 mph	Yes	Dry conditions only	£700-900
Yuneec Q500 Typhoon	1.1 kg	0.5 kg	25 mins	600 m	54 mph	Yes (12MP)	Dry conditions only	£900-1,100 (RTF)
SkyJib-X4 XL Ti-QR	15 kg	7.5 kg	15 mins	3,000-25,000 m	24 mph	Yes	Wind	£7,500-8,000
Altura Zenith ATX8	3.1 kg	2.9 kg	45 mins	1,000 m	44 mph	Yes	Light rain/snow	£15,000-20,000
MicroDrones MD4-1000	2.65 kg	1.2 kg	88 mins	5,000 m	26 mph	Yes	Light rain/snow	£20,000-30,000

Weather proofing

Most low-end and mid-level commercial UAVs have limited operating conditions. The ability to operate in a broader range of weather conditions, such as high winds, rain and snow, is generally found in the more expensive commercially available drones, as weather hardening adds weight, which has cost implications. Compared to military-grade UAVs, such as AeroVironment's Puma AE (All Environment) model, commercial UAVs have a limited ability to operate in harsh, unpredictable and extreme climatic environments. Commercial UAV users could retrofit weather hardening to drones, though the extra weight would likely reduce flight time and payload capacity unless power or the number of rotors was also increased.

Imaging

Most UAVs have medium- to high-resolution cameras (at least 12 megapixels) and the ability to capture both stills and video. The use of a gimbal can allow manual and electronic camera rotation, providing greater situational awareness. Civilian UAV operators can install LiDAR and infrared cameras on UAVs.

Automated and programmable piloting and Follow Me settings

Most commercially available drones can be set to fly a predetermined flight path based on GPS coordinates (fly-by-wire). Newer models also have Follow Me autopilot settings that enable the UAV to automatically follow the operator.

Unmanned ground vehicles

Unmanned ground vehicles have been available for several decades. The simplest example, as reportedly used by Islamic State (IS) in Iraq, is the familiar remote controlled car. At the other end of the spectrum, the first fully-autonomous road vehicles for the commercial market and advanced military robotics are being developed.

There are two categories of UGVs. The first are remote controlled vehicles piloted by humans who are in full control of the vehicle but driving it from a distance. These include the Modular Advanced Armed Robotic System (MAARS) used by the US Army. The second are autonomous drones that drive themselves

using algorithms, sensor inputs and pre-set waypoints. These include the Mobile Detection Assessment and Response System (MDARS) used by the US Army and Navy, and the Google Self-Driving Car Project.

UGVs have a large range of applications – from hobbyists using remote controlled cars for entertainment and leisure to the military using vehicles capable of operating in dangerous regions and environments, including for disarming explosives.

For the hobbyist, commercially available small remote controlled cars can travel up to 35 mph over rough ground, cost between £40 and £1,200, and can drive for 15 to 90 minutes over relatively short distances. They tend to have very limited payloads but could be customised to include cameras. In contrast, the military and defence sector use of UGVs is well established and increasing. This includes vehicles such as the RipSaw, a commercially available UGV the US Army equipped with weapons and used in Iraq. The Ripsaw is priced at approximately \$250,000 (£165,000) and is capable of driving at up to 95 mph, carrying a 900 kilogram payload. The US Army used over 6,000 UGVs in Iraq and Afghanistan for ISR missions and counter-IED tasks.⁶ South Korea is also reportedly using stationary armed surveillance 'robots' in the demilitarised zone along the border with North Korea. While there is limited commercial availability of military-grade UGVs, variants of models such as the I-Robot 110 and Mil-Sim A5 Robotic Weapon may enter a broader commercial market in the future.

Due to the wide range of variations and capabilities, it would be possible to customise or purchase a UGV capable of carrying either explosive payloads or cameras for relatively modest prices and logistical difficulty. However, it is worth noting that a comparable manned vehicle would be significantly cheaper.

Specifications affecting hostile UGV operations

There are only a limited number of UGV specifications affecting operations that are applicable to all classes of UGV. The diversity in technological capabilities makes pinpointing operational limitations challenging.

⁶ <http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=186583>.

Mobility and speed

UGVs can move across ground terrain in a range of modes and vehicle configurations. There is an important relationship between the ability of a UGV to move across diverse all-terrain environments, such as hills, obstructions, semiaquatic or flooded areas and uneven surfaces, and the speed with which a vehicle can move. For example, the average remote controlled car may have a reasonably high top speed but be unable to traverse uneven terrain very well. On the other hand, counter-IED UGVs with caterpillar tracks have a far greater capacity to negotiate diverse terrains but at much lower speeds.

Imaging

UGVs, particularly smaller vehicles that operate low to the ground, provide only limited situational awareness to operators, particularly in contrast to UAVs. Without telemetry systems, navigation based solely on video stream is likely to significantly limit the effectiveness of some UGVs. While UAVs provide superior visual situational awareness from a distance, UGVs fitted with more advanced environmental sensors, such as thermal imagers and chem-bio sensors, may offer operators a more

thorough understanding of on-the-ground environments.

Payload

The payload capacity of UGVs varies widely. As with most types of unmanned vehicles, there are obvious speed and mobility to payload weight trade-offs. In most instances, a commercial UGV or remote controlled car will have a higher payload capacity than hobbyist UAVs, but the UAV operator has greater visual awareness and manoeuvrability.

Range

Most remote controlled UGVs have limited range, though higher end models used by special operation forces are likely to be tailored for specific missions. Ranges for counter-IED and bomb disposal operations are likely to be based on average blast radius. For models used in hazardous material inspection or site contamination, a range of one kilometre should be sufficient to protect the operator. The range a hostile operator will require is dependent on the level of risk they are willing to expose themselves to depending on the target. In reality, the effective range is also dependent on the type of terrain the vehicle has to travel over to reach its target.

Table 2: Select list of UGVs

Model	Weight	Operating environment	Range	Max speed	Camera	Components	Price
Happy Cow 777-270 i-Spy	166 g	Limited	30 m	n/a	HD video/still camera	None	£30
Jumpshot MT	n/a	All terrain	100-200 m	27 mph	No	n/a	£175
Savage XL Octane RTR	7 kg	All terrain	100-200 m	36 mph	No	n/a	£775
Mil-Sim A5 Robotic Weapon	90 kg	All terrain All weather	215-500 m	50 mph	IR/low lux with night vision	Armed with lethal or non-lethal munitions	£2,500-6,500
I-Robot 110 First Look	2.5 kg	All terrain All weather Waterproof	200 m	3 mph	4 built-in cameras (front, rear and side-facing)	Can add specialised cameras, thermal imagers, chem-bio sensors and charge deployment accessories	£13,000-£15,000
MATILDA (Mesa Associates' Tactical Integrated Light-Force Deployment Assembly)	28 kg	All terrain All weather	1,200 m	2 mph	Pan-tilt zoom camera	68 kg payload capacity with adaptable configurations: sensor, attack and manipulate	£15,000
Modular Advanced Armed Robotic System (MAARS)	136 kg	All terrain All weather	800-1,000 m	7 mph	Drive and gunnery cameras with thermal imaging	Armed with lethal or non-lethal munitions	n/a

Unmanned marine vehicles

Unmanned marine vehicles are available in two main classes: underwater and surface platforms. The majority of UUVs fall into the first category. These underwater vehicles are designed for two principal commercial applications: marine research and offshore oil and gas sector activities. The 2014-15 search for missing Malaysia Airlines flight MH370 demonstrated a further novel application of UUVs for search and recovery. The Association for Unmanned Vehicle Systems International (AMVSI) has identified over 745 UUV platforms, with an estimated 75% in some stage of development, manufacture or deployment.⁷ In 2013, there were 115 active UUV platforms available in the United Kingdom.⁸

The market for UUVs is smaller than the UAV market, as it lacks the high levels of hobbyist uptake and is far more reliant on commercial usage. The civilian market is restricted by the very limited capabilities of lower priced entry-level models. However, expensive drones with broader capabilities are becoming more readily available. The cost of an advanced underwater UUV can reach more than £1 million. UUVs in this price range have the ability to travel at a depth of 4,500-6,000 metres for up to 28 hours and over a distance of 100 miles.⁹ Market research from March 2014 estimated that the global market for remotely-operated and autonomous UUVs would be £1.08 billion that year, growing to £3.15 billion by 2019.¹⁰

The two key operational attributes of underwater UUVs are range and dive depth, with cheaper models requiring a cable connection in order to dive below the surface. Most underwater drones have a limited payload (less than 10 kilograms) because of the need to remain buoyant, and are used for visual or sonar imaging and collection of scientific

data. Surface UUVs are dependent on speed, payload and range (a 'control triangle' comparable to the naval architects' 'iron triangle' of speed, payload and endurance).¹¹ They are capable of carrying up to 1,000 kilograms of explosives, such as was used in the non-drone attack on the USS Cole in October 2000 in Yemen.

Cheaper drones and those operating nearer to the surface are controllable by Wi-Fi up to a range of 300 metres, giving a pilot direct control over the drone. However, the majority of high-end submersible models move using a GPS-based system of waypoints. It is still possible for a pilot to maintain some level of control by changing the drive-to GPS coordinates or depth levels via acoustic messages and satellite communication; however, this form of control is limited at best, and the pilot could not, for example, navigate a submersible drone through a confined space. Due to the high cost and variable commercial use, underwater marine drones tend to be highly customisable. Features such as the basic outer shell, navigation, energy and propulsion components, and payloads, such as cameras or sonar equipment, are customisable.

Specifications affecting hostile UUV operations

There are several factors that affect UUV operations. Typically, higher-cost drones feature significantly greater payload capacity, imaging capability, range and depth than lower-cost drones.

Payload

Payload capacity is affected by two factors: internal space and the buoyancy of the drone. A payload that is above the buoyancy weight will cause the drone to sink at a rate proportional to the weight variance. A payload below the buoyancy can be offset by the drone's navigation facilities, including filling the buoyancy tanks to achieve a neutral level. Any space left in the payload chamber of underwater UUVs can be filled with high buoyancy foam to increase the potential payload weight. Higher-end UUVs will have more space for packages as well as higher natural buoyancy levels. The entry level drones may lack any payload capacity.

7 <https://higherlogicdownload.s3.amazonaws.com/AUVSI/b657da80-1a58-4f8f-9971-7877b707e5c8/UploadedFiles/AUVSIUMVCoreCapabilities08-08-13.pdf>. Note, the remaining 25% of platforms are either inactive (10%) or insufficient information is available to determine production or operational development (15%).

8 <https://higherlogicdownload.s3.amazonaws.com/AUVSI/b657da80-1a58-4f8f-9971-7877b707e5c8/UploadedFiles/AUVSIUMVCoreCapabilities08-08-13.pdf> (p. 5).

9 http://www.ths.org.uk/documents/ths.org.uk/downloads/shallowwater_auv_and_usv.pdf.

10 <http://www.prnewswire.com/news-releases/unmanned-underwater-vehicles-market-worth-484-billion-by-2019-252903011.html>.

11 http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR384/RAND_RR384.pdf.

Speed

Speed is determined by the engine output and the shape and weight of the craft. The engine output of underwater models is very low, with top speeds in the region of 3-6 mph (similar to jogging speed). The higher end of the market is more focussed on delivering endurance rather than speed. In contrast, speed is key factor for surface drones, which can reach speeds of up to 30 mph.

Imaging

Imaging technology tends to be placed into the payload chamber in UMVs. This can range from scientific instruments measuring changes in pressure or water quality, to sonar equipment and visual capabilities. The latter allows drones to be used for surveillance or reconnaissance of critical infrastructure, such as oil rigs or offshore military equipment, including naval vessels.

Range

The range of a drone is not determined by controller range if the UMV is capable of satellite or GPS communication. If this is the case, provided the drone remains in contact with the GPS network, the range is determined by the fuel capacity (generally electric batteries) and optimal speed. A drone able to travel at 3 knots (3.45 mph) for 25 hours has an effective range of 86.25 miles. If GPS communication is not possible, the drone is typically limited to either Wi-Fi controller ranges (typically up to 300 metres) or a physical cable connecting it to a pilot (typically less than 100 metres long).

Depth

Due to the pressure placed on a vehicle that descends under the water and the hazards of water damage on electrical components, the shell of a drone determines the depth to which it can travel. Drones with shells made of higher strength metals, such as titanium, are able to travel deeper than those made of cheaper metals or plastics. Depth is not a factor when UMVs are deployed against surface targets, but some critical infrastructure targets have significant depth, such as oil lines and platforms or communications cables.

Table 3: Select list of surface UMVs

Model	Weight	Payload	Fuel capacity	Max speed	Camera/ sonar	Price
C-Target 3	325 kg	0 kg	40 litres	28.7 mph	Yes	£POA
AutoNaut 3.5	120 kg	40 kg	20 litres (plus solar panels)	3.45 mph	Yes	£POA
AutoNaut 5	230 kg	130 kg	20 litres (plus solar panels)	4.6 mph	Yes	£POA

Table 4: Select list of submersible UMVs

Model	Weight	Buoyancy	Operation time	Range	Depth	Max speed	Camera/ sonar	Estimate price
HydroView Pro 5M	6.4 kg	0.9 kg	180 mins	0.046 miles	100 m (attached to cable)	4.6 mph	Yes	\$10,000-15,000 (£6,500-9,700)
Remus-100	37 kg	1 kg	600 mins	51.8 miles	100 m	5.18 mph	Yes	\$250,000 (£163,000)
Bluefin-21	750 kg	7.3 kg	1,500 mins	86.25 miles	4,500 m	3.45 mph	Yes	\$2.5 million (£1.63 million)

A review of the known use of drones by various

Assessment of known drone use by non-state actors

terrorist, insurgent, criminal, corporate and activist threat groups around the world has identified two principal categories of hostile use: attack and intelligence gathering. There are particular concerns that that drones will be used as simple, affordable and effective airborne Improvised Explosive Devices (IEDs). Governments are also concerned by the decentralisation and democratisation of intelligence, surveillance and reconnaissance (ISR) capabilities made possible by the widespread availability of drones. In contrast, this is a development that is welcomed by activists working to hold governments and corporations to account. A brief summary of the review is presented in the following pages. The majority of drones used are unmanned aerial vehicles, as they are more readily commercially available and offer more options than land- or sea-based platforms.

Lone wolf

There are many examples of individuals using drones for purposes beyond authorised and accepted use, and these suggest scenarios for future lone wolf attacks.

In September 2011, a 26-year-old American man was arrested by undercover FBI agents planning to fly explosives-laden model aeroplanes into the Pentagon and US Capitol and rig mobile phones to detonate improvised explosive devices (IEDs). In January 2015, an off-duty employee of the US National Geospatial-Intelligence Agency lost control of a friend's DJI Phantom quadcopter, which then crashed onto the White House lawn. The incident raised concerns about the extent to which the Secret Service is prepared for drone activity. Four months later, a man was arrested for trying to fly a Parrot Bebop drone over the White House fence. In France, unidentified drones have been flown over the US embassy, the Eiffel Tower, the Invalides military museum, the submarine communications base at Sainte-Assise, the Place de la Concorde, the Elysee Palace and multiple nuclear power stations. In June 2014, an unidentified drone was used to monitor the French national football team during a closed training session at the 2014 World Cup in Brazil. In July 2014, an unidentified drone came within six metres of an Airbus A320 as it landed at London's Heathrow Airport, prompting the Civil Aviation Authority to issue new safety guidelines, known as the 'dronecode'. In October 2015, an unidentified drone crashed into the Sydney Opera House.

Fortunately, there has so far been very few instances of individual terrorists using drones to undertake attacks. What could be was demonstrated in April 2015 when a man landed a drone on the Japanese prime minister's office in Tokyo. The drone was carrying a bottle containing radioactive sand from Fukushima, which was emanating up to 1.0 microsievert per hour.

In a response to a freedom of information request by Open Briefing, the Metropolitan Police Service revealed that between January 2013 and August 2015, 20 suspicious drone related incidents had been recorded in and around London.¹² Sixty per cent of the disclosed incidents related to air navigation orders where civil aviation requirements had

¹² https://www.whatdotheyknow.com/request/counter_drone_measures#incoming-702249.

been breached; the rest related to criminal or illegal activity. In one case, a UAV was used to smuggle drugs into a prison and in another case a drone was flown over 200,000 people on 20 December 2014.

Terrorist organisations

The Lebanon-based militant group Hezbollah has the longest history of drone use by a non-state group. Hezbollah reportedly maintains a small fleet of UAVs, including Iranian Ababil and Mirsad platforms and their Hezbollah derivatives.¹³ Some reports estimate that the fleet includes upwards of 200 platforms for ISR and combat missions.¹⁴ In November 2004, Hezbollah allegedly flew an Iranian UAV over parts of northern Israel before returning to Lebanese territory. In August 2006, Hezbollah launched three small Ababil drones, some allegedly carrying explosive payloads, with the intention of attacking Israeli military targets. The drones were shot down by Israeli F-16s. In October 2012, Hezbollah allegedly flew a small Ayub drone 35 miles into Israeli airspace with the intention of undertaking reconnaissance on a nuclear reactor. An Israeli aircraft shot the drone down before it returned to Lebanon.

More recently, it is possible that Hezbollah has more consistent access to Iranian UAVs, including the Ababil-3, and are using UAVs against al-Nusra Front fighters in Lebanon. In September 2014, the Fars News Agency reported that Hezbollah had achieved its first successful drone strike, killing an estimated 23 'Syrian rebels'.¹⁵ In April 2015, IHS Jane's published evidence of a Hezbollah UAV airfield in the northern Bekaa Valley, Lebanon, that included a UAV ground command station.¹⁶ The group is thought to be continuing to use UAVs for ISR in the border region between Syria and Lebanon.

Al-Qassam Brigades, the military wing of the Palestinian organisation Hamas, is suspected of having a small fleet of UAVs and a crude production workshop. During Operation Protective Edge in 2014, Israeli forces shot

down a potentially armed Hamas-controlled Arbabil-1 UAV with a Patriot surface-to-air missile. Al-Qassam Brigades advised that the drone was only one of three that breached Israeli airspace, though the Israeli military deny this claim. In December 2014, a drone flyover of a Hamas military parade resulted in Israel scrambling fighters that returned to base after the drone did not enter Israeli airspace.

More recently, Al-Qassam Brigades announced that it had captured an Israeli Skylark 1 that came down in Gaza in July 2015. The group claimed that the drone had been repaired and was operational. Al-Qassam Brigades also claims to have developed three UAV platforms, two with combat payloads and one for surveillance.

The extremist militant group Islamic State were shown to be using DJI Phantom UAV platforms in Fallujah, Iraq, from early 2014. While the early demonstrations of commercially available drones appeared to be for propaganda purposes only, there is emerging evidence that these platforms are now providing actionable ISR and target acquisition capabilities to Islamic State.¹⁷ There are some indications that IS used hobbyist drones to gain situational awareness ahead of the campaign to capture the Tabqa military airfield in northern Syria in August 2014. In March 2015, US military forces launched an airstrike against an IS militant who had been flying a UAV over Fallujah. In April 2015, Islamic State released a video showing UAVs being used for reconnaissance and battlefield coordination during its assault on the Baiji oil refinery complex in Iraq.¹⁸ In May 2015, the Kurdish Peshmerga shot down an IS drone that had been filming their positions. In August 2015, there were reports that Kurdish soldiers had captured a remote controlled car carrying explosives that had failed to detonate. In the same month, US Central Command released a list of airstrike targets around the world, including 'an ISIL drone' near Ramadi in Iraq.¹⁹

There are significant barriers to planning and carrying out a major terrorist attack of any sort. The intelligence work carried out by the

¹³ <https://medium.com/war-is-boring/this-new-airstrip-could-be-home-to-hezbollah-s-drones-bdec97ff36a8>.

¹⁴ <http://www.ynetnews.com/articles/0.7340.L-4457653.00.html>.

¹⁵ <https://www.youtube.com/watch?v=gUSGNAP19XQ>.

¹⁶ <http://www.janes.com/article/50922/hezbollah-airstrip-revealed>.

¹⁷ <https://medium.com/war-is-boring/islamic-state-has-drones-7827987c1755>.

¹⁸ <http://www.longwarjournal.org/archives/2015/04/islamic-state-uses-drones-to-coordinate-fighting-in-baiji.php>.

¹⁹ <http://www.centcom.mil/en/news/articles/august-3-military-airstrikes-continue-against-isil-terrorists-in-syria-and>.

British security services provides a robust line of defence against terrorist groups. There have been no known examples in the United Kingdom, Europe or the United States of terrorist organisations using drones for either attack or intelligence gathering. However, Islamic State is reportedly obsessed with launching a synchronised multi-drone attack on large numbers of people in order to recreate the horrors of 9/11.

Insurgent groups

Insurgent groups have many of the same capabilities and intentions as terrorist organisations, but do not face the same regulatory and law enforcement barriers to attacks on British interests as groups attempting to use drones to launch attacks within the United Kingdom. Drones therefore have the potential to become significant components of insurgents' armouries. Obtaining aerial, ground and marine reconnaissance and attack capabilities would mark a step change for many insurgent groups.

Donetsk People's Republic (DPR) militias in eastern Ukraine reportedly possess and deploy sophisticated Russian-made Eleron-3SV drones for ISR campaigns. In contrast, the Ukrainian military has been using a range of modified and tailor-made hobbyist UAVs for ISR support. There are reports that the DPR militias are using signal jamming and GPS spoofing countermeasures against some Ukrainian drones; however, more advanced autopilot software in the tailor-made models is more resilient against these countermeasures. The Ukrainians have requested US military drones, such as Reapers, and jamming equipment and radar to better intercept the Russian-made drones.

In August 2002, a Colombian Army unit allegedly discovered remote-controlled aeroplanes during a raid on a Revolutionary Armed Forces of Colombia (FARC) camp. The intended use of the aircraft remains unclear.

Organised crime groups

Mexican drug trafficking organisations (DTOs) have been documented using drones to smuggle illicit drugs across the US-Mexican border since 2010. The US Drug Enforcement Administration (DEA) has recorded around 150 drone trips across the border since 2012.

Nearly two tonnes of cocaine and other drugs are estimated to have been trafficked into the United States in this way, with an average of 13 kilograms of drugs per shipment.²⁰ In January 2015, a drone that crashed in Tijuana, Mexico, was carrying over three kilograms of methamphetamine. In August 2015, two men pleaded guilty to trafficking 12 kilograms of heroin across the US-Mexican border in the first cross-border seizure involving a drone.

In the face of increasingly successful military and law enforcement operations against illicit drug smuggling in the early 1990s, Colombian drug cartels began to invest in producing narco-submarines as an alternate to small planes and go-fast boats. In August 2005, US authorities captured an unmanned semi-submersible in the Pacific Ocean. This was a torpedo-style cargo container, rather than a self-propelled vessel, which was towed underwater behind a boat and released if a patrol ship was spotted. The narco-torpedo would then release a buoy with a location transmitter system so that it could be retrieved later. In July 2010, the Ecuadorian police and navy found a jungle shipyard containing a 22.5-metre long narco-submarine. The advanced 'supersub' had a camouflaged hull made of Kevlar and carbon fibre and a cargo bay capable of holding over eight tonnes of cocaine. The high level of sophistication apparent in the various captured narco-submarines and the huge resources available to the DTOs means that it is highly likely that they are now investing in remotely-piloted submersible vessels in addition to custom-made UAVs.

Corporations

There have been isolated examples of drones being used to obtain commercially sensitive information, such as drones flying over the filming of Game of Thrones in Ireland, Apple's new campus site being built in Cupertino in the United States and the BAE Systems facility in northern England that builds submarines for the Royal Navy. However, there have been no documented examples of corporations using drones for commercial advantage or espionage. However, there is a broad range of threat scenarios whereby drones are integrated into corporate espionage operations alongside cyber offensives and

²⁰ <http://www.insightcrime.org/news-briefs/mexico-s-cartels-building-custom-made-narco-drones-dea>.

spear phishing campaigns. A likely scenario involves using drones as a means to deploy a malware payload over specific Wi-Fi networks. The leaked emails of Italian spyware vendor Hacking Team suggest that early concept plans for using drones for airborne malware delivery over Wi-Fi networks were being discussed with Insitu, a division of Boeing.²¹

One offensive scenario is the use of crowd control drones by British companies against strikers or demonstrators threatening foreign operations. An example of such a drone is the Desert Wolf Skunk, which is equipped with four high-capacity paint ball barrels that can fire a variety of ammunition, including pepper spray balls and plastic balls. The drones can be flown in formation by a single operator. In what the South African company calls a 'life threatening situation', each drone can fire 80 balls per second, allowing for 'real stopping power'.²² Desert Wolf reportedly sold 25 Skunks to an international mining company after a photo of the drone was featured on a military news website in May 2014.

Activist groups

Although clearly not presenting a threat of the same type or magnitude as the other threat groups discussed in this briefing, activists have employed drones to support their political campaigns on a number of occasions. In September 2013, the German political party the Pirate Party flew a Parrot quadcopter towards the German chancellor, Angela Merkel, during a campaign rally in Dresden.²³ The stunt was in protest against the German government's surveillance policies. In October 2014, Greater Albania activists flew a drone carrying the Greater Albania flag over an Albania-Serbia football match.²⁴ Greater Albanian's claim territory from Albania's neighbours, including Serbia. In July 2015, Women on Waves delivered pregnancy termination pills by drone from Germany to Poland to highlight restrictive abortion laws in Poland. Animal rights activist

groups have used UAVs to remotely capture farming, animal husbandry and animal testing practices in the United States. In April 2015, a man protesting over the Japanese government's nuclear energy policy landed a drone containing radioactive sand on the roof of the Japanese prime minister's office in Tokyo.

Although the use of drones by activists is still uncommon, the most likely way in which drones will be used by such groups in future is in undertaking publicity-seeking exercises in front of the media or filmed using onboard cameras. Activists could also use drones to assist existing campaign efforts through reconnaissance and surveillance.

²¹ <https://theintercept.com/2015/07/18/hacking-team-wanted-infect-computers-drone/>.

²² <http://www.desert-wolf.com/dw/products/unmanned-aerial-systems/skunk-riot-control-copter.html>.

²³ <https://www.youtube.com/watch?v=WcFiMCMbUHo>.

²⁴ <https://www.youtube.com/watch?v=hJSQf737Agw>.

There are two theatres in which non-state actors could use drones as either an offensive weapon against the United Kingdom and its interests or as an intelligence gathering tool:

1. **The international theatre**, consisting of all British military operations, embassies and commercial sites and operations abroad. These are vulnerable to attack by terrorist or insurgent groups or to being targeted by activist groups protesting against government policy or the actions of British corporations.
2. **The domestic theatre**, consisting of critical national infrastructure, military sites, government buildings and tourist sites within the United Kingdom. These are vulnerable to terrorist attacks, disruption by activist groups or corporate espionage.

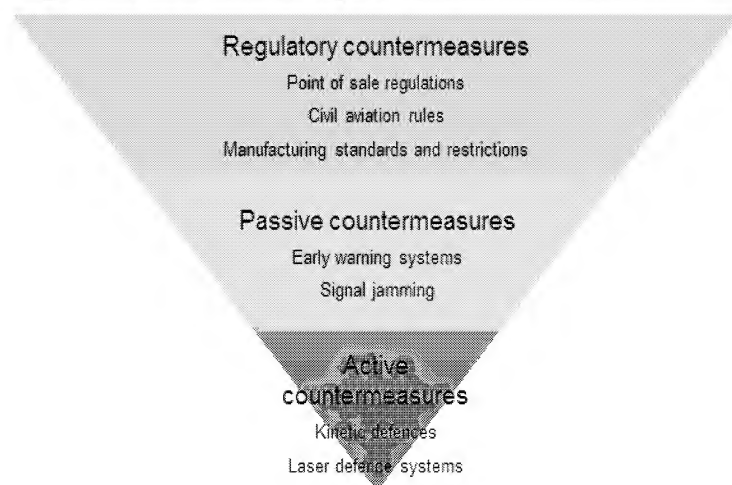
There are three key defence scenarios, which range from easier to target/ easier to defend to harder to target/harder to defend:

1. **The long-term static target**, such as a foreign embassy or nuclear power station.
2. **The temporary static target**, such as a G7 summit or a speech by a politician.
3. **The mobile target**, such a military supply convoy or the prime minister's car.

The UK government, police, military and security services will need to introduce countermeasures to reduce or mitigate the risk of commercially available drones being used for attack or ISR operations. These countermeasures need to be proportionate to the risk, economically and operational sustainable and balance interests relating to privacy, individual freedoms, safety and commercial interest.

Drones are a unique technology providing users with significant capabilities. Defence system against illegal or harmful use of unmanned

Figure 1: The hierarchy of countermeasures



vehicles should provide for 'all hazard' scenarios and multiple threat environments. However, time and resource investments should be prioritised for countermeasures that respond to the scenarios with highest risk (high likelihood/high impact).

No single countermeasure is completely effective at limiting the hostile use of drones by non-state actors. The best strategy is therefore to employ a hierarchy of countermeasures encompassing regulatory countermeasures, passive countermeasures and active countermeasures. A high-level evaluation of the various countermeasures that are available is provided in the following pages. The focus is on unmanned aerial vehicles, as they present the greatest threat, but many of the countermeasures can be applied to unmanned ground and marine vehicles too, and where applicable countermeasures specific to these vehicles have also been considered.

Regulatory countermeasures

Domestic regulations can put in place a range of measures targeting the full supply chain and life cycle use of drones. Regulations would need to proportionate and balance a range of competing safety and commercial demands, including establishing procurement barriers for threat actors while at the same time encouraging innovative commercial use and maintaining easy access to suitable platforms for hobbyists. Specific regulatory countermeasures may include:

- Point of sale regulations, including identification requirements for the purchase and sale of drones above a certain level of capability.
- Civil aviation rules and licensing regimes to regulate the use of drones, with harsh penalty regimes for flying near critical national infrastructure and sites of national security importance.
- Manufacturing standards and restrictions for UAVs, including no-fly zones built in to firmware and limits on carrying capacity and controller range.

Procurement and import regulations

The main international regulation relating to drones is the 1987 Missile Technology Control Regime (MTCR). The regime currently has

34 members, and the UK government is a founding member. The MTCR aims 'to restrict the proliferation of missiles, complete rocket systems, unmanned air vehicles, and related technology for those systems.' It is a voluntary association of countries that share the goal of 'non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction.'²⁵

Regulations to stop the procurement and import of drones to the United Kingdom only cover those weighing more than 20 kilograms or are equipped to undertake any form of surveillance or data acquisition at time of purchase. Heavier drones require airworthiness approval and those capable of surveillance are more stringently regulated. This limited regulation means that drones weighing less than 20 kilograms can be imported without license, despite many drones weighing 5-20 kilograms being capable of carrying explosives or camera equipment; for example, the SkyJib-X4 XL Ti-QR weighs 15 kilograms and can carry a payload of 7.5 kilograms.

Civil aviation regulations on UAV licensing and use

There are currently 32 countries using regulations to control the use of drones domestically, particularly unmanned aerial vehicles. The scope and scale of the regulations range from altitude or weight limits to a complete ban on all unmanned aerial vehicles. Regulation in the United Kingdom is limited. Drones of any size or weight are permitted, though they must be used within the visual sight line of the pilot. In general, UAVs cannot be flown above 400 feet in altitude without special permission and must remain clear of controlled airspace without Air Traffic Control permission. Commercial operation requires a license, which is given to an operator for a particular class of UAV (small fixed wing or small multirotor).²⁶

In contrast, some countries maintain a complete ban, while others have stringent rules similar to those in effect in South Africa. South Africa has a well-developed series of regulations on UAVs, with some of the strictest rules in the world short of an outright ban. The operators of drones must have a valid remote

²⁵ <http://www.mtcr.info/english/>.

²⁶ <https://www.caa.co.uk/default.aspx?catid=1995&pageid=16012>.

pilot license and drones cannot be operated without a letter of approval from the director of the South African Civil Aviation Authority, which is valid for 12 months. Drones must not be flown near nuclear power plants, prisons, police stations, crime scenes, law courts, critical national infrastructure or strategic installations. Regulations also prohibit drones from being flown in formation or swarm, flown directly overhead or within a lateral distance of 50 metres of a person or crowd, or within 50 metres laterally of any structure or building.²⁷

There is a vigorous debate between the innovators, users and regulators. The former argue for a more laissez faire approach to allow the rapid development of the civilian drone market. They argue that if the rules of use become restrictive now, this could smother the sector before it properly established. Conversely, others argue that if the rules are too relaxed there is a high probability of misuse with potentially disastrous consequences. As usual, a compromise needs to be found.

Firmware limitations

The Chinese UAV producer DJI has built safety features into the firmware (the permanent software programmed into read-only memory) used by its drones. The firmware maintains several No Fly Zones based on the GPS coordinates of the pilot's location. There are around 350 No Fly Zones worldwide.²⁸ These zones are primarily designed to keep drones away from airports. Furthermore, within eight kilometres of a no-fly zone, the pilot is unable to set an automatic fly-to waypoint, forcing them to remain in manual control of the drone near these zones.

The No Fly Zone is currently a limited-use tool implemented to protect airports; however, legislation could be implemented to extend the measure to protect other key sites. In January 2015, DJI reported that it is considering implementing such a zone over Washington DC after one of their drones crashed onto the lawn of the White House. In theory, the firmware updates to protect these sites could be hacked and bypassed, but this would require specialist knowledge not likely to be held by most solo attackers at least. The company is also working

to prevent criminals from using workarounds to circumvent such security features.

This would make it very difficult for individuals without the technical knowledge of computer programming and the criminal links to illegally import drones to be able to acquire and fly drones near sites that have been marked as needing protecting. In effect, this limits the lone wolf terrorist, and sends a clear message to activists and businesses of what the legal and illegal uses of drones are.

Passive countermeasures

Early warning systems

There are several early warning systems that can identify a drone within a defined area. Traditional technology such as radar and CCTV can be effective, but new commercial systems are being developed that specifically alert operators to the presence of drones. Such commercial systems include:

DroneShield is developing a system that contains a database of common acoustic signatures unique to drones. If a drone is detected, DroneShield instantly alerts security officers via text message, email or through an existing alarm system. The system was deployed at the 2015 Boston Marathon. DroneShield technology is also available for cars and vans, allowing a VIP convoy to implement such a detection system.

Domestic Drone Countermeasures is developing personal and commercial detection systems that can detect radio frequency transmitters and triangulate moving transmitters. The system consists of a primary command and control module that can communicate with radio frequency sensor nodes up to 60 metres away, with each node typically able to detect drones within 15 metres in all directions.

Dedrone has developed the DroneTracker multi-sensor detection system, which uses an array of sensors to detect civilian drones in real time. The system uses microphones, a daylight camera and an infrared camera to track drones within a 100 metre radius, which can be extended by deploying the units in series.

²⁷ <http://www.thedroneinfo.com/south-africa-drone-regulations/>.

²⁸ <http://theuavdigest.com/uav036-no-fly-zones-for-uavs/>

Although commercial systems have the potential to be very effective against civilian drones, military-grade systems include electronic warfare and radar capabilities that make them far more effective against advanced drones. As the counter-drone market grows, defence companies may begin offering scaled down versions of their military systems for use by businesses and high-net-worth individuals.

A comprehensive early warning system would use a combination of acoustic detectors, thermal imaging sensors, cameras and radar. This would allow a drone to be detected, tracked and identified by target sites. However, many sites lack sophisticated detection capabilities, such as radar, and it would be costly to install them. Companies such as a Dedrone are developing cost-effective and drone-specific alternatives. In some high-value targets, such as military bases or Whitehall, radar could be installed, but investing in commercial systems alone would be sufficient for most sites.

Signal jamming

Once an early warning system detects a drone, popular drone control frequencies can be blocked around the target using a radio frequency jammer, such as the RCJ40-D or PRO45 High Power (civilian) or JAM201 or GM20 (military). It is also possible to block these frequencies at all times, though this would make mobile phone communications in and around the site difficult. However, a drone user can use a wireless intrusion prevention system to alert them to attempted jamming. Advanced radio receivers can use a multi-spectrum frequency set that alternates through little used frequencies meaning that the receiver is harder to block. Military-grade jammers can block a wider spectrum of frequencies. However, frequency jamming is illegal in the United Kingdom without permission.

By implementing no-fly zones around critical infrastructure, any drone detected can be assumed to be malicious and the controller frequencies could be blocked. However, if a threat actor is able to hack the firmware to override the inbuilt no-fly zones, they could place GPS waypoints within the defensive perimeter. If the drone was detected and controller frequencies were blocked, the

drone operator would be unable to change the coordinates or have any control over the aircraft; however, the drone would continue along its pre-determined route and still be able to strike a static target. What controller frequency blocking does is remove the threat actor's ability to guide the drone onto a mobile target or target of opportunity or to take evasive action against any active defence systems. GPS jamming is also needed in order to interfere with the GPS radio signal or undertake a spoofing attack to change the drone's perceived coordinates and either take control of the vehicle or cause it to crash land.

A possible alternative method for taking control of a drone was revealed in January 2015 when a security researcher claimed to have developed the world's first drone malware: Maldrone. The Python script is loaded to the drone over a local Wi-Fi network and can turn off the drone's autopilot system and take control remotely.²⁹ However, drone malware is currently very limited, and requires the specific model of the targeted drone to be known. The Maldrone demonstration does offer an idea of what might one day be possible though.

Active countermeasures

Kinetic defence systems

For those drones that remain a threat after the controller frequency and GPS have been blocked, the last barrier of defence in the hierarchy of countermeasures are systems capable of destroying hostile drones. This includes kinetic weapons, such as missiles, rockets and bullets.

Israel's Iron Dome air-defence system has been tested for its counter-UAV capabilities, and according to some sources can destroy armed drones before they are in attack range. Less-advanced kinetic defences use rockets or bullets and require line of sight, meaning a drone can get much closer to the target. All kinetic systems present a risk of collateral damage if deployed in a populated area. Missiles and rockets fired at UAVs could cause catastrophic damage if they miss their target. If the drone is hit, shrapnel and wreckage could still cause casualties on the ground. The blast radius from a missile or rocket fired at a UGV could include civilians near the targeted drone, and bullets fired at UGVs could easily strike

29 <http://garage4hackers.com/entry.php?b=3105>.

passersby.

Less risky commercial options include non-lethal projectile weapons that fire blunt force rounds, such as bean bags or rubber bullets, or small portable net guns that can ensnare drones. A consortium of British companies called Liteye has developed the Anti-UAV Defence System (AUDS) system that can detect and track drones using electronic scanning and radar then disrupt its operation with a brief, focused broadcast of directional radio frequency jamming.

Laser defence systems

Laser defence systems are being developed that have less chance of causing causing collateral damage than kinetic systems. For example, a Chinese consortium of companies, led by the China Academy of Engineering Physics, has developed a weapon system that can shoot down light drones at low altitude using a 10 kilowatt high energy laser. It has a 1.2-mile range and is effective against aircraft travelling at up to 112 mph and at a maximum altitude of 500 metres. It can destroy the drone within five seconds of locating its target. Boeing is developing the truck-mounted High Energy Laser Mobile Demonstrator for the US Army and the Compact Laser Weapons System, which can be assembled in 15 minutes and destroy a drone in 15 seconds.

Laser defence systems are still in development. However, once deployed and combined with an early-warning system, directed energy weapons could provide a useful counter to a hostile drone, particularly if radio frequency jammers and GPS jammers have also been deployed to remove the pilot's ability to operate the drone. In this situation, the laser defence system would be working against an autonomous vehicle, making it easier to lock-on to and destroy. However, such systems might be of limited use in built-up areas, as they can only engage drones during times of line of sight, which may not be enough time to destroy the drone before it reaches its target. The fastest commercially available drones can travel at around 50 mph, meaning a drone could travel 112 metres in the five seconds a laser would take to destroy it. In a domestic, urban setting, this makes such systems most suited to the defence of static targets with clear lines of sight.

Conclusions and policy recommendations

It is estimated that around 200,000 civilian-use drones are being sold worldwide every month.³⁰ Although they are currently expensive, ever-more advanced drones capable of carrying sophisticated imaging equipment and significant payloads are readily available to the civilian market. Unmanned aerial vehicles currently present the greatest risk because of their capabilities and widespread availability, but developments in unmanned ground and marine vehicles are opening up new avenues for hostile groups to exploit.

A range of terrorist, insurgent, criminal, corporate and activist threat groups have already demonstrated the ability to use civilian drones for attacks and intelligence gathering. The best defence against the hostile use of drones is to employ a hierarchy of countermeasures encompassing regulatory countermeasures, passive countermeasures and active countermeasures.

Regulatory countermeasures can restrict the capabilities of commercially available drones and limit the ability of hostile groups and individuals to procure and fly drones. However, any new regulations controlling drones should be targeted and proportionate to the threat. The key specifications affecting drone operations are payload capacity, range, speed, depth (for UMVs), weather proofing, imaging and autopilot settings. Policymakers should pass stricter regulations limiting the capabilities of commercially available drones in the key specifications affecting hostile drone operations, particularly payload capacity. Particular attention should be paid to limiting the attack and ISR capabilities of UAVs and the attack capabilities of surface UMVs. Manufacturers should be required to install firmware that includes the GPS coordinates of no-fly zones around sensitive fixed locations. This would automatically shut down drones approaching these sites, thereby restricting malicious use. Finally, civilian operators of drones capable of carrying payloads should be licenced and the serial numbers of purchased drones registered.

Passive countermeasures alert security to the presence of any drone within a no-fly zone or defensive perimeter around a static or mobile target. They limit the ability of hostile groups and individuals to guide a drone onto a mobile target or target of opportunity or take evasive action against any kinetic defences. The military has advanced systems that can track and destroy drones using radar, lasers and electronic warfare; however, the market for commercial and civilian early warning systems is at a nascent stage of development. The British government should support the research and development of commercial multi-sensor systems capable of detecting and tracking drones within a target area. The government should also make funding available to police forces and specialist units for the purchase of early warning systems and other passive drone countermeasures, including radio frequency jammers and GPS jammers. Radio frequency jammers are heavily restricted in the United Kingdom; however, such equipment could provide additional protection and security to vulnerable locations and individuals by blocking command signals to drones. Therefore, the government should relax the regulations restricting the use of radio frequency jammers for protection against hostile drone use around defined key sites.

30 <http://dronelife.com/2015/01/24/drone-sales-figures-2014-hard-navigate/>.

Active countermeasures can be deployed against drones that still represent a threat despite passive systems being employed. However, the active countermeasures currently available for use in non-military settings are limited. Kinetic weapons – missiles, rockets or bullets – can be very effective, but present considerable risks of collateral damage if used in urban civilian areas. Less risky defences include laser systems or non-lethal projectile weapons and net guns, but these may not successfully destroy a hostile drone and require line of sight, which may be difficult in heavily built-up areas. Despite these limitations, the British government should support the research and development of innovative less-lethal anti-drone systems, such as directional radio frequency jammers, lasers and malware, and set out clear guidelines for the police and military use of kinetic weapons against hostile drones as a last line of defence.

With active countermeasures still under development or presenting a high risk of collateral damage, the focus should be on the swift adoption of appropriate regulatory and passive countermeasures and increased funding for the research and development of effective active countermeasures. The most effective and cost efficient measures should be prioritised. The implementation of more expensive countermeasures for low likelihood/high impact events involving drones will depend on the government's risk appetite with regards to specific potential civilian, government or military targets. Combined with high-quality intelligence on the present threat of the hostile use of drones by various threat groups, the recommendations outlined in this report represent the best chance of countering the new and evolving threat from the hostile use of drones by non-state actors.

However, such countermeasures are not foolproof. Furthermore, there is also the very real chance that, as with drones themselves, countermeasures will be deployed in turn by some threat groups against British police or military drones. The technology of remote-control warfare is impossible to control; the ultimate defence is to address the root drivers of the threat in the first place.

Remote Control Project

Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)207 549 0298
media@remotecontrolproject.org

www.remotecontrolproject.org

Open Briefing

27 Old Gloucester
Street London
WC1N 3AX
United Kingdom

+44 (0)20 7193 9805
info@openbriefing.org

www.openbriefing.org



GENDARMERIE ROYALE DU CANADA • ROYAL CANADIAN MOUNTED POLICE

BULLETIN DE L'ÉQUIPE NATIONALE DES INFRASTRUCTURES ESSENTIELLES

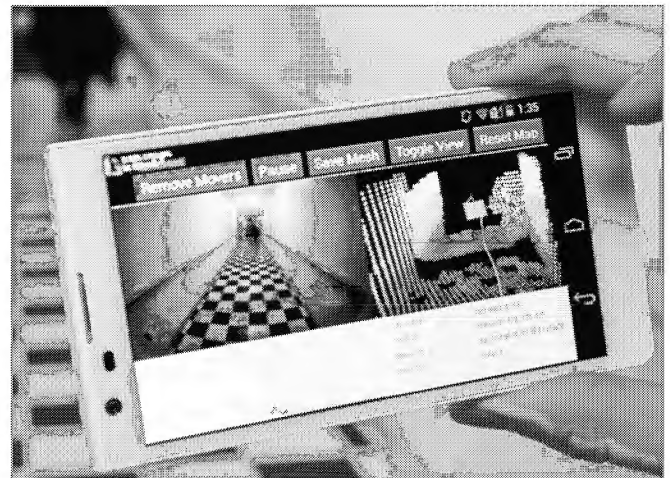
SENSIBILISATION DES AGENTS:

2016-01-20

À l'appui de la stratégie adoptée par le gouvernement du Canada pour assurer la résilience des infrastructures essentielles (IE), la Gendarmerie royale du Canada (GRC) évalue et signale l'information relative aux menaces et à la criminalité dirigées contre les IE canadiennes. Ces renseignements ou ces éléments d'information peuvent servir à protéger les IE du Canada. L'information contenue dans le présent bulletin date du **20 janvier 2016**. Les membres des organismes d'application de la loi font partie du secteur de la Sécurité et les militaires font partie du secteur des administrations publiques. Le gouvernement du Canada considère que ces deux secteurs sont des secteurs d'IE.

CONTEXTE

Le projet Tango de Google vise à changer radicalement la façon dont les téléphones intelligents et les tablettes interagissent avec leur environnement. Google a conçu un appareil mobile doté de capteurs et de caméras tournés vers l'extérieur qui sont capables de faire un balayage des espaces et des objets environnants. Le prototype pourrait effectuer 250 000 mesures par secondes. Le résultat : un écran qui affiche des graphiques en trois dimensions extrêmement détaillés qui reproduisent avec précision les spécifications exactes des espaces et des objets à l'échelle humaine (échelle 1:1). Les graphiques affichés à l'écran ne sont pas statiques. Les capteurs de suivi du mouvement de l'appareil détectent plutôt les déplacements de l'utilisateur dans l'espace et ils peuvent



Opérations criminelles de la Police fédérale

Ce document appartient à la Gendarmerie royale du Canada (GRC), Programme de sécurité nationale. Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable de la Sous-direction des affaires criminelles relatives à la sécurité nationale, GRC

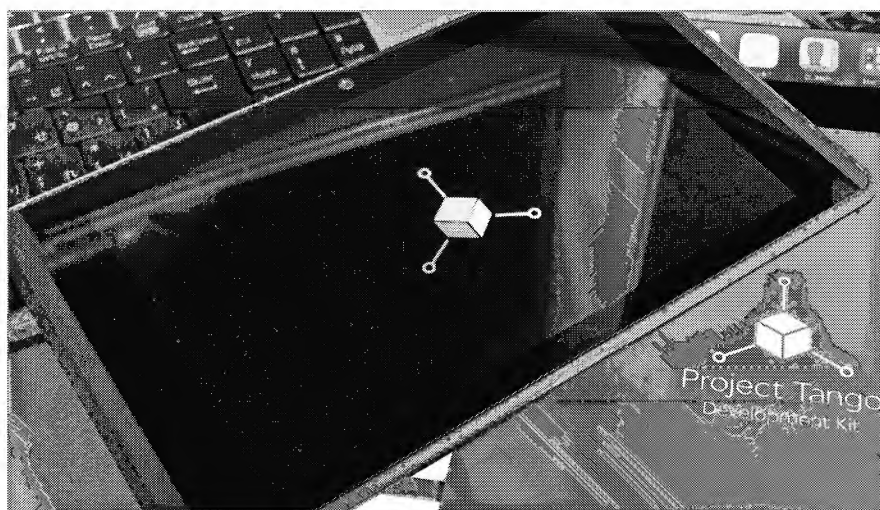
adapter les graphiques à 360 degrés en fonction de l'emplacement ou de la position de l'utilisateur.

Cette technologie permet aux utilisateurs :

- de se déplacer dans des immeubles publics (p. ex. un centre commercial, un terminus ou une aéroport) pour localiser rapidement ce dont ils ont besoin ou l'endroit où ils veulent se rendre;
- d'obtenir rapidement des mesures exactes dans un espace donné;
- de reconnaître et de tirer parti de nouveaux endroits après avoir reçu des photos par courriel;
- d'enregistrer des cartes en 3D d'espaces intérieurs pour les examiner plus tard.

Il est possible d'effectuer toutes ces fonctions sans avoir besoin d'un GPS ou d'autres signaux externes.

Le 7 janvier 2016, une entreprise chinoise de haute technologie, Lenovo, a annoncé qu'elle développait le premier téléphone intelligent équipé de la technologie Tango, qui sera offert aux consommateurs à l'été 2016 au coût de 500 \$. Google a déjà lancé sa trousse de développement sur tablette pour le projet Tango, qui est principalement destinée aux développeurs de logiciels. Il est possible d'acheter cette trousse en ligne¹ au coût de 500 \$ et celle-ci est expédiée sans frais. Au mois de juin 2015, plus de 3000 de ces trousse sur tablette avaient été vendues. À ce jour, le seul appareil équipé de la technologie Tango de Google est la tablette Yellowstone de sept pouces (photo ci-dessous).



Opérations criminelles de la Police fédérale

Ce document appartient à la Gendarmerie royale du Canada (GRC), Programme de sécurité nationale. Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable de la Sous-direction des affaires criminelles relatives à la sécurité nationale, GRC

ÉVALUATION

Opérations criminelles de la Police fédérale

Ce document appartient à la Gendarmerie royale du Canada (GRC), Programme de sécurité nationale. Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable de la Sous-direction des affaires criminelles relatives à la sécurité nationale, GRC



INDICATEURS DE COMPORTEMENT

RECOMMANDATIONS

L'ENIE encourage les destinataires du présent document à signaler à leur service de police local toute activité suspecte ou criminelle. Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité qui pourrait menacer la sécurité nationale du Canada, communiquez avec :

Opérations criminelles de la Police fédérale

Ce document appartient à la Gendarmerie royale du Canada (GRC), Programme de sécurité nationale. Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable de la Sous-direction des affaires criminelles relatives à la sécurité nationale, GRC



Réseau info-sécurité nationale : 1-800-420-5805
Service canadien du renseignement de sécurité (SCRS) : 613-993-9620

Rédigé par : Équipe nationale des infrastructures essentielles
Opérations criminelles de la Police fédérale
Courriel : SIR-SIS@RCMP-GRC.GC.CA

¹ https://store.google.com/product/project_tango_tablet_development_kit?hl=fr

Opérations criminelles de la Police fédérale

Ce document appartient à la Gendarmerie royale du Canada (GRC), Programme de sécurité nationale. Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable de la Sous-direction des affaires criminelles relatives à la sécurité nationale, GRC



RCMP-GRC



ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA



BULLETIN DE L'ÉQUIPE NATIONALE DES INFRASTRUCTURES ESSENTIELLES

MISE À JOUR : EXTRÉMISTES INTERNES (EMPLOYÉS) DANS L'INDUSTRIE DE L'AVIATION

2016-02-10

À l'appui de la stratégie adoptée par le gouvernement du Canada pour assurer la résilience des infrastructures essentielles (IE), la Gendarmerie royale du Canada (GRC) évalue et signale l'information relative aux menaces et à la criminalité dirigées contre les IE canadiennes. Ces renseignements ou ces éléments d'information peuvent servir à protéger les IE du Canada. L'information contenue dans le présent bulletin date du **10 février 2016**. **Elle s'adresse essentiellement aux policiers, aux premiers intervenants et aux agents de l'application de la loi dans les aéroports ainsi qu'au personnel de sécurité des aéroports et des transporteurs aériens.**

PRINCIPALES CONSTATATIONS

- Cependant, en raison de la portée internationale de l'industrie aéronautique et de l'état général de la menace, les agents de l'application de la loi et le personnel de la sécurité doivent rester au courant des tendances et des techniques qui ressortent de dossiers internationaux connus concernant des travailleurs de l'aviation.
-
-

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



CONTEXTE ET LIMITES

En 2013, l'ENIE a présenté une évaluation des tendances et techniques dégagées de cas d'extrémisme connus dans le secteur de l'aviation.

(Prière de se reporter aux annexes A et B pour un guide et des sommaires illustrés.)

ÉVALUATION

-

la portée internationale de l'industrie aéronautique et de l'état général de la menace, les agents de l'application de la loi et le personnel de la sécurité doivent rester au courant des tendances et des techniques qui ressortent de dossiers internationaux connus concernant des travailleurs de l'aviation.

- Selon les données, les complots d'attentats extrémistes confirmés orchestrés par des employés d'aéroports ou de transporteurs aériens ont connu un faible taux de

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



réussite qui s'explique par le fait que les autorités sont parvenues à détecter et à déjouer la plupart d'entre eux.¹

comme une tactique efficace qu'il vaut la peine d'adopter ou de remployer dans l'avenir. Devant un tel scénario, il devient de plus en plus primordial de détecter et de signaler les comportements suspects.

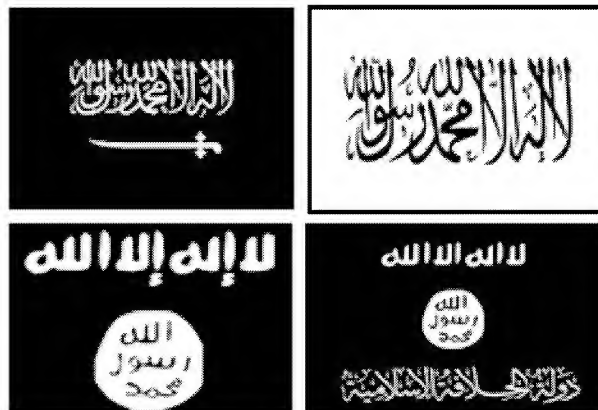
INDICATEURS DE COMPORTEMENT

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



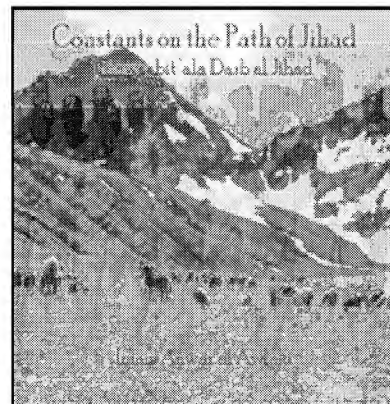
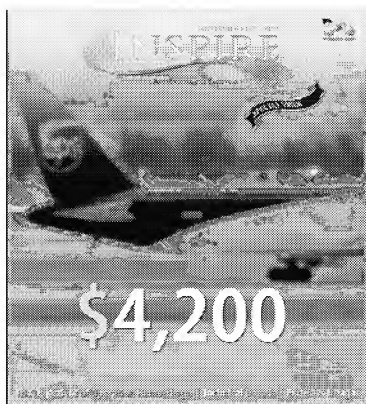
ii) Cas de radicalisation possibles



Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.





MESURES D'ATTÉNUATION POTENTIELLES



Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



RECOMMANDATIONS

L'ENIE encourage les destinataires du présent document à signaler tout renseignement concernant des activités criminelles ou suspectes aux organismes d'application de la loi de leur région. Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité qui pourrait menacer la sécurité nationale du Canada, communiquez avec :

Réseau info-sécurité nationale au 1-800-420-5805
Service canadien du renseignement de sécurité (SCRS) au 613-993-9620

Rédigé par : Équipe nationale des infrastructures essentielles
Opérations criminelles de la Police fédérale
Courriel : SIR-SIS@RCMP-GRC.GC.CA

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



ANNEXE B ~ SOMMAIRES DE CAS D'EXTRÉMISME CONFIRMÉS ET SOUPÇONNÉS DANS LE SECTEUR DE L'AVIATION

- Le vol 159 de Daallo Airlines a quitté l'aéroport international Aden Adde de Mogadiscio, en Somalie, le 2016-02-16. Selon des sources, un présumé kamikaze est monté à bord de l'aéronef et, 15 minutes après le décollage, a fait sauter un explosif dont la déflagration a laissé une ouverture dans le fuselage. La vidéo de surveillance prise avant le départ montrerait deux hommes remettant ce qui semble être un ordinateur portatif au présumé kamikaze après le passage de celui-ci par la sécurité. Au moins un de ces deux hommes serait un employé de l'aéroport; il porte un gilet de sécurité de haute visibilité orange. Au moins 20 personnes ont été arrêtées en lien avec l'explosion. À part le kamikaze, tous les passagers ont eu la vie sauve. Le gouvernement somalien a confirmé qu'il s'agissait d'un acte de terrorisme organisé.



- Selon des médias grand public citant des sources proches de l'enquête des autorités égyptiennes sur l'écrasement du vol 9268 de MetroJet en octobre 2015, quatre individus ont été détenus en lien avec l'affaire. L'avion s'est écrasé dans la péninsule du Sinaï après son décollage de l'aéroport international de Charm el-Cheikh; les 224 personnes à bord ont péri. Plusieurs experts ont confirmé qu'un engin explosif en était la cause. Peu de temps après l'accident, le groupe EIIS a revendiqué l'attentat. Un technicien d'Egypt Air, dont le cousin aurait adhéré au groupe EIIS, est soupçonné d'avoir posé l'engin à bord du vol. Selon des sources, le technicien ainsi que le bagagiste soupçonné de l'avoir aidé à poser l'engin dans l'avion ont été détenus. Deux policiers travaillant dans l'aéroport ont également été placés en détention.
- Terry Loewen**, 58 ans, technicien en avionique, a été arrêté en 2013 pour avoir apparemment planifié de faire exploser un véhicule-bombe sur l'aire de trafic de l'aéroport Mid-Continent de Wichita (Kansas), où il travaillait, à proximité d'aérogares et d'aéronefs de passagers. En utilisant sa carte d'accès d'employé pour se rendre sur l'aire de trafic tôt un matin de décembre, il aurait cru qu'il infligerait un maximum de dommages physiques, économiques et matériels en perpétrant l'attentat juste avant les vacances de Noël, l'une des journées les plus achalandées de l'année.

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



Selon des documents judiciaires, Loewen se serait livré aux activités suivantes : étudié l'agencement de l'aéroport et pris des photos des points d'accès; consulté les horaires de vol; aidé à obtenir des composants de l'engin explosif et parlé de sa détermination à déclencher l'engin explosif et à devenir un martyr. Il a été condamné à 20 ans d'emprisonnement.

- **Belal Sadallah Khazaal** a travaillé comme bagagiste pour Qantas pendant 12 ans (de 1988 à 2000). Pendant ces années, il a attiré l'attention des autorités australiennes. Selon un rapport de la CIA, Khazaal aurait suivi en 1998 une formation dans un camp militaire en Afghanistan et serait devenu un confident pour des dirigeants d'al-Qaïda. On a trouvé un guide de 110 pages rédigé par Khazaal expliquant comment fabriquer des bombes, comment perpétrer un assassinat ou un enlèvement et comment descendre un avion en vol. Un tribunal a jugé que le guide visait à faciliter la commission d'actes terroristes. En 2009, Khazaal a été condamné à 12 années d'emprisonnement.
- **Rajib Karim** a travaillé comme concepteur de logiciels pour British Airways (BA) de 2007 à son arrestation en 2010. Pendant le procès, la poursuite a fait valoir que Karim avait délibérément cherché à se placer à BA pour pouvoir conseiller des terroristes au Yémen, au Pakistan et au Bangladesh sur des aspects particuliers des dispositifs de sécurité dans les aéroports, sur les liquides permis et sur les questions que les agents de l'immigration posent aux voyageurs. Pendant qu'il travaillait à BA, Karim échangeait des courriels avec Anwar Al-Awlaki, qui était alors un membre dirigeant d'al-Qaïda dans la péninsule arabique. Al-Awlaki a ordonné à Karim de recruter des collègues qui pourraient savoir comment contourner les détecteurs à rayons X de l'aéroport. Après quoi Karim s'est rapproché d'un bagagiste et d'un employé de la sécurité à l'aéroport Heathrow. Karim a aussi offert de profiter d'une éventuelle grève du personnel de BA pour devenir agent de bord à titre temporaire. En 2011, Karim a été condamné à 30 années d'emprisonnement.
- **Samina Malik** travaillait dans une boutique côté piste à l'aéroport Heathrow. En 2006, elle communiquait par courriel avec l'extrémiste condamné Sohail Qureshi. Ce dernier a admis avoir planifié un attentat terroriste à l'étranger, peut-être contre

From: "Khan Inqilabi" <@hotmail.com>
 To: @hotmail.co.uk
 Subject: salams
 Date: Sun, 08 Oct 2006 11:12:54 +1400

Salams...

Sis, i hope u get this email before anyone else does...

Wat is the situation like at work? Is the checking still very harsh?or have things cooled down a bit?

bara' Allah feek...

ws wr wb

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



les troupes britanniques en Afghanistan. Selon la police, Malik a fourni à Qureshi de l'information sur les dernières mesures de sécurité mises en place à l'aéroport. Qureshi voulait apparemment sortir du pays incognito pour exécuter son opération à l'étranger. Avant d'essayer de partir, Qureshi a écrit à Malik : « Ma sœur, j'espère que tu auras ce courriel avant quelqu'un d'autre. À quoi ressemble le système au travail? Les vérifications sont-elles toujours aussi rigoureuses ou les choses se sont-elles calmées un peu? ... Supprime le message après l'avoir lu! » Dans sa réponse, Malik a décrit en détail les mesures de sécurité, notamment les procédures de palpation sommaire et de vérification des liquides. Elle a signé : « Une étrangère dans l'attente de devenir une martyre. » Parmi les articles dans les bagages de Qureshi, on a trouvé un manuel de formation d'AQ, des lunettes de vision nocturne et des manuels militaires canadiens et américains dans lesquels on fait référence à des tactiques d'intervention et de combat en zone urbaine.

- **Asmin Amin Tariq** est l'une des 24 personnes qui ont été arrêtées relativement au complot d'attentat aux liquides explosifs de 2006 qui visait dix vols transatlantiques. Avant d'être arrêté, Tariq travaillait comme garde de sécurité pour Jet Airways à l'aéroport Heathrow, aussi il avait accès en tout temps à tous les secteurs de l'aéroport. Selon la US Transportation Security Administration, Tariq a aidé des extrémistes islamistes à se faire passer pour des employés de l'aéroport afin de mener à bien leur reconnaissance des dispositifs de sécurité à Heathrow. De plus, Tariq aurait fourni de l'information sur les procédures de sécurité de l'aéroport à de futurs poseurs de bombes potentiels.
- **Arid Uka** travaillait au bureau de poste du Terminal 2 de l'aéroport de Francfort. Le 2011-03-02, il est sorti du terminal et s'est approché d'un autobus. Après s'être assuré qu'il transportait des militaires américains en partance pour l'Afghanistan, il est monté à bord et a tiré neuf coups de feu avec un pistolet, tuant le chauffeur et un soldat. Deux autres soldats ont été blessés. Selon des sources publiques, l'un des éléments déclencheurs de la tuerie d'Uka a été le visionnement d'un extrait d'un film de fiction où des soldats



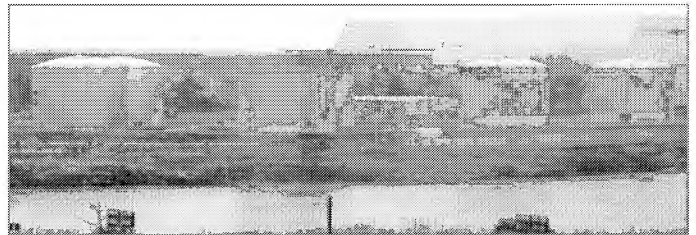
Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



américains se livraient à un viol. En 2012, Uka a été condamné à l'emprisonnement à perpétuité.

- **Gregory Patterson**, converti à l'Islam, travaillait en 2005 dans une boutique hors-taxes à l'aéroport international de Los Angeles (LAX). Il était l'un des quatre agents recrutés par un groupe extrémiste installé en Californie, Jami'iy yat Ul-Isla Is Saheeh (JIS), qui voulait attaquer le comptoir des billets du transporteur aérien El Al à l'aéroport. Selon l'entente sur le plaidoyer du cerveau de l'opération Kevin James, le défendeur a écrit une lettre en mars 2005 à son coconspirateur Levar Washington lui disant que Patterson devrait garder son emploi à l'aéroport. Patterson a fait de la reconnaissance et des recherches en ligne sur El Al. Il a aussi acheté une carabine et s'est pratiqué au tir, et a appris à fabriquer des explosifs artisanaux. Il a été condamné à douze ans et demi d'emprisonnement.
- **Russell Defreitas** a travaillé comme manutentionnaire de fret à l'aéroport international JFK, puis comme superviseur des stagiaires d'une compagnie de fret jusqu'à ce qu'il soit mis à pied en 2001. Defreitas était le cerveau derrière le complot de 2007 visant les réservoirs et les pipelines de distribution de carburant aviation à l'aéroport international JFK. Selon des conversations enregistrées et un informateur du FBI, Defreitas aurait dit que ses connaissances uniques de l'aéroport et de ses vulnérabilités seraient très utiles pour faire progresser l'attentat. Selon des documents judiciaires, Defreitas a dit à ses conjoints qu'à plusieurs reprises il avait testé les dispositifs de sécurité en place à JFK en volant des marchandises. Defreitas aurait filmé et pris des photos de l'aéroport pour aider à repérer des cibles, tiré des images de Google Earth du secteur ciblé, étudié la sécurité de l'aéroport et planifié la fuite après l'attentat. En 2011, il a été condamné à l'emprisonnement à perpétuité.
- De 1997 à 2002, **Adem Yilmaz** a été garde de sécurité pour la compagnie ferroviaire Deutsche Bahn à la gare régionale de l'aéroport de Francfort. Cette gare est située sous le Terminal 1 de l'aéroport. Membre de l'Union du jihad islamique, Yilmaz faisait partie d'une cellule de quatre personnes qui avait d'abord envisagé de cibler l'aéroport de Francfort. Après un certain temps, le complot d'attentat s'est tourné vers d'autres cibles en Allemagne, y compris des Américains expatriés et la base des forces aériennes américaines de Ramstein. En 2010, Yilmaz a été condamné à 11 années d'emprisonnement.



Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



- **Muhammad Syahrir** a travaillé comme technicien d'aéronef pour la ligne aérienne nationale d'Indonésie, Garuda. La police croit qu'il a infiltré Garuda pour les besoins d'un vaste complot dirigé contre le transporteur aérien. Membre du Jamaah Islamiyah affilié à AQ, Syahrir aurait été un redoutable fabricant de bombe et participé aux attentats à la bombe perpétrés en 2009 contre des hôtels d'Indonésie. Il a été tué dans une descente policière.

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



NOTES DE FIN DE TEXTE

¹ "EXTRÉMISTES INTERNES (EMPLOYÉS) DANS L'INDUSTRIE DE L'AVIATION : TENDANCES ET TECHNIQUES", ERIE, GRC, 2013-05-01.

Federal Policing Criminal Operations

Ce document appartient au Programme de sécurité nationale de la Gendarmerie royale du Canada (GRC). Il est expressément prêté à votre organisme à titre confidentiel et aux fins d'usage interne seulement. Il ne peut être reclassifié, copié, reproduit, utilisé en tout ou en partie ou diffusé à un plus large auditoire sans le consentement de l'auteur. Il ne peut être utilisé dans des affidavits, des procédures judiciaires ou des citations à comparaître ou encore à toute autre fin juridique ou judiciaire sans le consentement de l'auteur. Le traitement et l'entreposage de ce document doivent respecter les directives établies par le gouvernement du Canada pour le traitement et l'entreposage des renseignements classifiés. Si votre service ne peut pas appliquer ces lignes directrices, veuillez lire le document et le détruire. La présente mise en garde fait partie intégrante de ce document et doit accompagner tous les renseignements qui en sont extraits. Si vous avez des questions au sujet des renseignements ou de la mise en garde, veuillez communiquer avec l'officier responsable des Opérations criminelles relatives à la sécurité nationale. GRC.



RCMP • GRC



ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA



BULLETIN DE L'ÉQUIPE NATIONALE DES INFRASTRUCTURES ESSENTIELLES

2016-07-15

À l'appui de la stratégie adoptée par le gouvernement du Canada pour assurer la résilience des infrastructures essentielles (IE), la Gendarmerie royale du Canada (GRC) évalue et signale l'information relative aux menaces et à la criminalité dirigées contre les IE canadiennes. Ces renseignements peuvent aider à protéger les IE du pays. Les évaluations de l'Équipe nationale des infrastructures essentielles (ENIE) visent à fournir aux intervenants concernés une évaluation des renseignements sur les enjeux liés à la protection des IE. L'information figurant dans la présente évaluation est à jour au **15 juillet 2016**.

PRINCIPALES CONSTATATIONS

-
-
-

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.



CONTEXTE

Le 2016-07-14, durant la fête nationale française à Nice (France), le conducteur d'un semi-remorque a foncé dans la foule venue assister aux célébrations sur la fameuse Promenade des Anglais.

Selon les témoins, le conducteur, qui roulait à environ 50 km/h, a zigzagué sur un tronçon d'environ 2 km de la Promenade afin de faucher le maximum de piétons avant d'échanger des tirs avec les policiers. Peu après, le conducteur a été abattu. L'attaque, qui serait l'œuvre d'un terroriste, aurait fait au moins 84 morts selon les autorités locales.



Source: Agence France-Presse

Les Services consulaires d'Affaires mondiales Canada ne rapportent aucun Canadien parmi les victimes. Selon l'agent de liaison responsable de la région, il n'y a pas de lien connu entre cette attaque et le Canada.

ÉVALUATION

i) Impact

Les précédentes évaluations de l'ENIE et de ses partenaires montraient que ce mode opératoire ne faisait jusque-là que très peu de victimes (environ un ou deux morts par attaque).

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.



À titre d'exemple, en l'espace de trois mois (d'octobre à décembre 2014), on a recensé six incidents impliquant le recours à un véhicule par des individus qui ont délibérément heurté des piétons, tuant six personnes et en blessant environ 45 autres. Ces attaques avaient été perpétrées au Canada (1), en France (2) et en Israël (3). (Voir le compte rendu complet à l'ANNEXE A.)



Source: New York Times

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.

ii) Accès

L'utilisation d'une semi-remorque plutôt qu'un véhicule personnel dans l'attaque perpétrée à Nice pose la question de savoir comment une personne malintentionnée pourrait se procurer un poids lourd.



S

Source: Twitter

iii) Incitation

Au moins trois organisations terroristes ont incité à commettre de telles attaques, à savoir l'État islamique (EI), le Hamas et al-Qaïda dans la péninsule arabique (AQPA). La propagande extrémiste regorge d'illustrations, dont des affiches et instructions publiées en ligne. (Voir le compte rendu complet à l'ANNEXE B.

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.

iv) Vulnérabilités

B – INDICATEURS POSSIBLES

Un indicateur à lui seul n'est pas nécessairement révélateur, mais l'observation de plusieurs des comportements ci-dessous chez un individu ou un groupe pourrait indiquer la préparation d'une attaque :

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.



Recommandations

Il est important que tous les partenaires, y compris les organismes d'application de la loi et le personnel de sécurité du secteur privé, signalent tout ce qui leur semble suspect. Le personnel de première ligne est le mieux placé pour observer les comportements suspects. Ils connaissent ce qui les entoure et savent ce qu'il est normal d'y trouver au quotidien. Un incident isolé peut sembler anodin, mais la conjonction de plusieurs incidents peut trahir une menace réelle.

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.



Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité qui pourrait menacer la sécurité nationale du Canada, communiquez avec :

le Réseau infosécurité nationale : 1-800-420-5805
le Service canadien du renseignement de sécurité (SCRS) : 613-993-9620

Rédigé par : l'Équipe nationale des infrastructures essentielles
Enquêtes criminelles de la Police fédérale
Courriel : SIR-SIS@RCMP-GRC.GC.CA

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.



ANNEXE A ~ INCIDENTS IMPLIQUANT DES VÉHICULES UTILISÉS COMME ARME (OCTOBRE À DÉCEMBRE 2014)

- Le 20 octobre 2014, vers 11 h 30 HNE, un homme seul, répondant au nom de Martin Couture-Rouleau, a percuté avec son véhicule deux membres des Forces canadiennes qui sortaient d'un café à Saint-Jean-sur-Richelieu (Québec). Un des soldats a été grièvement blessé et est par la suite décédé; le second a subi des blessures mineures. M. Couture-Rouleau a pris la fuite à bord de son véhicule et, pris en chasse par la police locale, a eu un accident à environ quatre kilomètres de là. Il est sorti de son véhicule, puis a été abattu après avoir menacé les agents d'un couteau. Il est mort à l'hôpital où on l'a transporté.
- Le 22 octobre 2014, peu après 18 h, un homme de 21 ans a foncé avec son véhicule dans une foule massée à un arrêt du train léger à Jérusalem, situé à proximité d'une voie de circulation achalandée. Un bambin a été tué et neuf personnes ont été blessées à leur sortie du train. L'automobiliste a été identifié par la police; il s'agit d'un terroriste palestinien connu du quartier Silwan à Jérusalem Est. L'homme a été abattu par les policiers et s'est éteint à l'hôpital.
- Le 5 novembre 2014, le chauffeur d'une minifourgonnette a foncé sur un groupe de plus de 12 personnes qui descendaient d'un tramway, sur l'itinéraire reliant les secteurs Est et Ouest de Jérusalem. Le chauffeur est ensuite sorti de son véhicule pour attaquer un groupe se trouvant sur la plate-forme, dont des policiers, à l'aide d'une barre de métal, avant d'être abattu par la police. Les autorités israéliennes estiment qu'il s'agit d'un attentat terroriste. Toujours selon les autorités israéliennes, l'homme, âgé de 38 ans, provenait d'un camp de réfugiés de l'Est de la ville et était partisan du Hamas, un groupe islamiste palestinien.
- Le 5 novembre 2014, Hamam Masalma, un membre du Hamas âgé de 23 ans, a foncé avec une fourgonnette commerciale portant une plaque d'immatriculation des autorités palestiniennes contre trois soldats israéliens se trouvant à une intersection en Cisjordanie. Les trois hommes ont été blessés.
- Le 21 décembre 2014, un automobiliste âgé de 40 ans a foncé dans la foule à Dijon (France) blessant quelque 11 personnes. Au moins une des victimes aurait été mortellement blessée. Le chauffeur, qui, selon les autorités, souffrait d'instabilité mentale, a été arrêté par la police après avoir ciblé des piétons à

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.

cinq endroits différents de la ville dans la nuit qui a suivi. Durant ce déchaînement qui a duré 30 minutes, le chauffeur aurait crié : « Allahu Akbar » (Dieu est grand) et qu'il agissait au nom des enfants de Palestine. Le procureur général de Dijon a mentionné que le chauffeur n'avait aucun lien connu avec des groupes terroristes de l'étranger et qu'il avait agi seul. Il était connu des services de police pour des incidents mineurs remontant à 20 ans et avait été interné dans un établissement psychiatrique à un moment donné.

- Le 22 décembre 2014, le conducteur d'une fourgonnette a foncé dans un marché bondé de clients qui faisaient leurs emplettes de Noël à Nantes, blessant dix d'entre eux. Le chauffeur se serait ensuite poignardé. Les autorités estiment qu'il s'agissait d'un acte délibéré, et ajoutent que le conducteur n'a invoqué aucun motif religieux ou politique, semblait agir seul et souffrait probablement de troubles mentaux. Les témoins ne s'entendent pas pour ce qui est de savoir si le conducteur a crié « Allahu Akbar » ou non.

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.

ANNEXE B ~ INCITATION DES GROUPES TERRORISTES À UTILISER DES VÉHICULES COMME ARME

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.



NOTES DE FIN DE DOCUMENT

² *Ibid.*

National Security Criminal Investigations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations Support Branch, RCMP.



RCMP-GRC



ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA



BULLETIN DE L'ÉQUIPE NATIONALE DES INFRASTRUCTURES ESSENTIELLES

SENSIBILISATION DES AGENTS :

Attaque au couteau dans un bureau de recrutement des Forces canadiennes à Toronto

2016-03-15

À l'appui de la stratégie adoptée par le gouvernement du Canada pour assurer la résilience des infrastructures essentielles (IE), la Gendarmerie royale du Canada (GRC) évalue et signale l'information relative aux menaces et à la criminalité dirigées contre les IE canadiennes. Ces renseignements ou ces éléments d'information peuvent servir à protéger les IE du Canada. L'information contenue dans le présent bulletin date du **15 mars 2016**. Les membres des organismes d'application de la loi et les militaires canadiens font partie du secteur de la Sécurité, que le gouvernement considère comme l'un des six secteurs d'IE au Canada.

CONTEXTE

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



ÉVALUATION DE L'ENIE

À l'heure actuelle, l'ENIE ne détient aucune information précise qui laisse croire à une menace imminente contre des installations ou le personnel policier ou militaire du Canada.

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



Une liste complète des attentats commis contre des organismes d'application de la loi et des militaires occidentaux figure à l'**ANNEXE A**.

FACTEUR À PRENDRE EN CONSIDÉRATION

(Des exemples précis figurent à l'**ANNEXE B**.)

Il est important que tous les partenaires, y compris les militaires, les organismes d'application de la loi et le personnel de sécurité du secteur privé, signalent tout ce qui leur semble suspect. Le personnel de première ligne est le mieux placé pour observer les comportements suspects.

L'ENIE encourage les destinataires du présent document à signaler à leur service de police local toute activité suspecte ou criminelle. Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité qui pourrait menacer la sécurité nationale du Canada, communiquez avec :

Réseau info-sécurité nationale : 1-800-420-5805
Service canadien du renseignement de sécurité (SCRS) : 613-993-9620

Rédigé par : Équipe nationale des infrastructures essentielles
Opérations criminelles de la Police fédérale
Courriel : SIR-SIS@RCMP-GRC.GC.CA

MANIPULATION DE RENSEIGNEMENTS

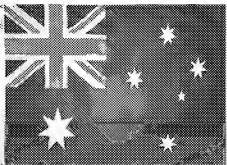

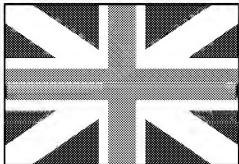

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



ANNEXE A - ATTENTATS COMMIS CONTRE DES ORGANISMES D'APPLICATION DE LA LOI ET DES MILITAIRES OCCIDENTAUX

LÉGENDE : **ATTENTATS RÉUSSIS** **COMLOTS RATÉS**

PAYS	TYPE D'ATTENTAT	RÉSUMÉ
		Le 2014-09-23 , Abdul Numan Haider, 18 ans, qui soutenait ouvertement l'EIL, est abattu après qu'il eu apparemment poignardé deux policiers à l'extérieur d'un poste de police en Australie. Le présumé assaillant avait accepté de rencontrer des membres d'un groupe anti-terroriste dans le cadre d'une enquête et s'était récemment fait retirer son passeport. Selon des sources ouvertes, la police faisait enquête sur lui en lien avec des allégations voulant qu'il ait déferlé un drapeau de l'État islamique dans un centre commercial de la banlieue.
		Le 2014-10-07 , quatre hommes dans la jeune vingtaine ont été arrêtés au Royaume-Uni lors d'un raid anti-terroriste. De plus, il semblerait que les hommes avaient des images, envoyées par Instagram, de deux policiers de la police métropolitaine de Londres et de deux agents de soutien à la police communautaire. La défense soutient que les hommes avaient l'intention d'abattre des policiers et des militaires dans les rues de Londres.

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).

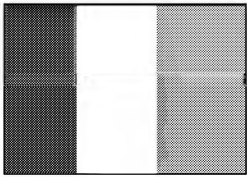

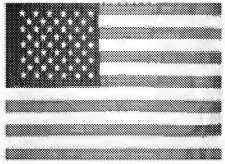

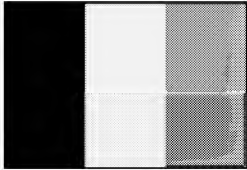

		<p>Le 2014-10-20, Martin Couture-Rouleau, âgé de 25 ans, a heurté à l'aide de son véhicule deux membres des Forces canadiennes alors qu'ils sortaient d'un café à Saint-Jean-sur-Richelieu (Québec). Selon les informations recueillies, Couture-Rouleau attendait, dans sa voiture en marche dans un stationnement d'un mail linéaire, d'apercevoir du personnel militaire. Il a pris la fuite à bord de son véhicule et, pris en chasse par la police locale, a subi une collision à environ quatre kilomètres de là. Il a quitté son véhicule, puis a été abattu après avoir menacé les agents d'un couteau.</p>
		<p>Le 2014-10-22, Michael Zehaf-Bibeau, âgé de 32 ans, a tué par balles un soldat canadien au Monument commémoratif de guerre du Canada à Ottawa avant de prendre d'assaut l'Édifice du Centre sur la Colline du Parlement. Il a été tué dans l'Édifice du Centre de la Colline du Parlement par les forces de sécurité.</p>
		<p>Le 2014-10-23, une escouade de quatre agents du service de police de New York effectuait une patrouille à pied dans un quartier de New York. Ils ont été attaqués par Zale Thompson, âgé de 32 ans. Une vidéo de l'incident montre un homme courant vers les policiers avec l'arme blanche, après être sorti de derrière un abribus non loin de là. Selon les médias, l'homme a brandi la hachette en direction de deux des agents qui, n'étant pas blessés, ont tiré en sa direction. Selon des sources ouvertes, Thompson avait un casier judiciaire en Californie et avait été renvoyé de la marine américaine pour inconduite.</p>
		<p>Le 2014-12-20, un Franco-Burundais, Bertrand Nzohabonayo (alias Bilal Nzohabonayo), aurait cogné à la porte d'un poste de police à Joué-lès-Tours (France). Lorsqu'un agent a ouvert, l'agresseur, âgé de 20 ans, lui a asséné un coup de couteau au visage. L'agresseur est ensuite parvenu à neutraliser et à blesser un second agent qui avait dégainé. Une agente a alors abattu l'agresseur d'un coup de feu. Selon la</p>

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).

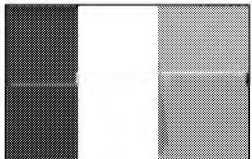

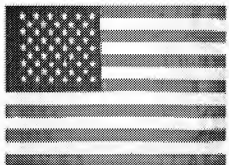

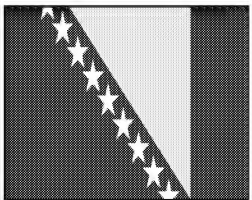

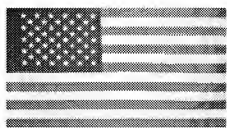

		police, Nzohabonayo aurait crié « Allahu Akbar » (Dieu est Tout-Puissant) durant l'agression.
--	--	---

		Le 2015-01-08 , Ahmedy Coulibaly, âgé de 32 ans, a abattu un policier municipal de la banlieue de Paris. Après avoir prêté allégeance à l'EIL, Coulibaly a lancé une série d'attaques devant coïncider avec le siège dans les bureaux de <i>Charlie Hebdo</i> à Paris.
		Le 2015-01-14 , Christopher Lee Cornell, âgé de 20 ans, a été arrêté par le FBI pour avoir comploté un attentat inspiré de l'EIL contre le Capitole, aux États-Unis, y compris des représentants du gouvernement et des policiers. Il voulait faire exploser des bombes tuyaux artisanales dans des immeubles gouvernementaux tout en tirant sur des hauts représentants américains. Il avait acheté des fusils semi-automatiques et 600 munitions avant de se rendre à Washington.
		Le 2015-01-16 , des individus soupçonnés de faire partie d'une cellule de 15 membres ont été arrêtés en Belgique et en France parce que les autorités affirmaient qu'ils avaient l'intention de tuer plusieurs policiers belges dans les rues et les postes de police. Diverses armes à feu, des uniformes de police, des explosifs et un couteau ont été saisis pendant le raid.

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

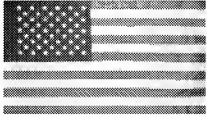

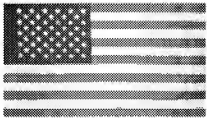

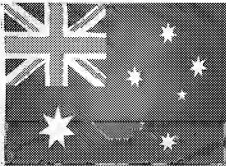

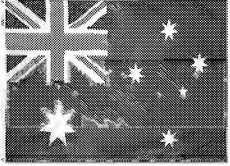

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).

		Le 2015-02-03 , Moussa Coulibaly, 31 ans, a attaqué au couteau trois soldats d'un groupe antiterroriste français à Nice, en France. Les soldats patrouillaient les bureaux d'une station de radio juive. Personne n'a été blessé gravement.
		Le 2015-03-26 , un spécialiste de la Army National Guard, Hasan Edmonds, et son cousin, Jonas Edmonds, 29 ans, ont été arrêtés par les autorités américaines pour avoir semble-t-il conspiré de fournir de l'équipement de soutien à l'EIL et de mener des attaques contre des installations militaires américaines en Illinois.
		Le 2015-04-27 , Nerdin Ibric, âgé de 24 ans, a crié « Allahu Akbar » (Dieu est tout-puissant) lorsqu'il a attaqué un poste de police à Zvornik, en Bosnie-Herzégovine. Un policier a été tué et deux autres ont été blessés. Selon les autorités bosniennes, Ibric est entré dans le poste de police armé d'un fusil automatique, puis a été abattu par la police après quelques échanges de coups de feu. Deux autres suspects, Avdulah Hasanovic, 24 ans, et Kasim Mehidic, 40 ans, ont également été arrêtés en lien avec cet attentat fatal. Hasanovic était sous enquête pour avoir semble-t-il aidé au recrutement de combattants pour l'EIL.
		En avril 2015 , Noelle Velentzas, 28 ans, et Asia Siddiqui, 31 ans, ont été arrêtées pour des attentats inspirés de l'EIL qu'elles voulaient mettre à exécution à New York. Les deux femmes avaient effectué des recherches approfondies sur la façon de concevoir un engin explosif et auraient eu en leur possession des bonbonnes de propane, du fertilisant et un exemplaire de <i>The Anarchist Cookbook</i> , un manuel qui fournit des instructions détaillées sur la manière de fabriquer des engins explosifs. Leur complot consistait à cibler des bases militaires et les funérailles de policiers du service de police de New York.

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

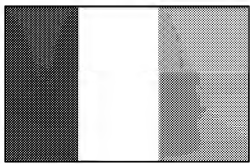

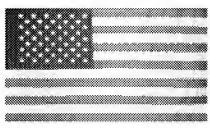

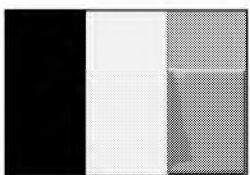

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).

		<p>Le 2015-04-10, John T. Booker Jr., âgé de 20 ans, a été arrêté par les autorités américaines pour avoir tenté de commettre un attentat-suicide inspiré de l'EIIL à l'installation militaire Fort Riley, au Kansas. Booker aurait tenté de brancher des fils à ce qu'il croyait être un engin explosif à l'intérieur d'un véhicule.</p>
		<p>Le 2015-07-16, Mohammad Youssef Abdulazeez a ouvert le feu dans un centre de recrutement militaire situé dans un mail linéaire à Chattanooga, au Tennessee. À bord d'une Ford Mustang décapotable louée de couleur argent, il a ouvert le feu au moyen d'un fusil AK-47. Il s'est ensuite rendu à un centre de la réserve navale, situé à sept miles de là, où il a ouvert le feu. Il a été abattu sur les lieux du deuxième endroit après avoir foncé dans une barrière. Il a tué quatre marins et en a blessé trois.</p>
		<p>En avril 2015, cinq adolescents ont été arrêtés pour avoir comploté de mener un attentat inspiré de l'EIIL contre des policiers aux événements d'Anzac Day tenus dans la ville de Melbourne, en Australie. Anzac Day est un jour national observé en Australie et en Nouvelle-Zélande pour honorer la mémoire de tous ceux qui sont morts au combat, que ce soit lors d'une guerre, d'un conflit ou d'une mission de paix. Le complot visait à attaquer des policiers et le public au moyen d'épées et de couteaux. L'Australian Security Intelligence Organization (ASIO) a fait savoir que les cinq adolescents avaient été ciblés par un recruteur de l'EIIL.</p>
		<p>Le 2015-10-02, Farhad Jabar Khalil Mohammad, âgé de 15 ans, a atteint d'une balle à l'arrière de la tête, à une distance rapprochée, un employé civil de la police de la Nouvelle-Galles-du-Sud (NGS). La victime, Curtis Cheng, âgé de 58 ans, sortait de l'immeuble du quartier général de la police par l'entrée principale vers 16 h 30 (heure locale), lorsque le tireur, qui se trouvait sur le</p>

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).

		trottoir vêtu d'un long vêtement noir, a tiré le coup de feu. Après ces événements, la police a perquisitionné la résidence de Mohammad et y a saisi des ordinateurs. Le 2015-10-03, la police de la NGS a confirmé que la fusillade était un acte terroriste, que Mohammad n'était pas connu des autorités et qu'il a fort probablement agi seul.
		Le 2016-01-07 , un homme a été abattu après avoir menacé des policiers à l'aide d'un couteau de boucherie à l'entrée d'un poste de police à Paris, en France. L'homme portait une fausse veste d'explosifs. La police a trouvé sur le corps de l'homme un téléphone cellulaire, un bout de papier où figurait l'emblème de l'EIIL et un bout de papier où une revendication de responsabilité était écrite en arabe.
		Le 2016-01-07 , Edward Archer, 30 ans, de Yeadon en Pennsylvanie, s'est approché d'une voiture de police dans le quartier de West Philadelphia et a tiré plusieurs balles à l'aide d'une arme de poing de 9 mm. Le policier a été atteint par trois balles mais a réussi à tirer sur le suspect. Ni le policier ni le suspect n'ont succombé à leurs blessures. Le suspect a déclaré qu'il avait agi « au nom de l'islam » et prêté allégeance à l'EIIL. Il possédait un casier judiciaire chargé.
		Le 2016-03-04 , une jeune Marocaine de 15 ans a été arrêtée pour avoir poignardé un policier qui s'était adressé à elle dans une gare en Allemagne. Le policier avait demandé à la jeune fille de lui montrer ses papiers d'identité, qu'elle lui a remis. Pendant que le policier lisait ses papiers, elle l'a poignardé au cou à l'aide d'un couteau de cuisine. L'attaque était inspirée de l'EIIL. Incapable de se rendre à l'État islamique, la jeune fille avait décidé d'attaquer une cible en Europe.

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).

ANNEXE B – INDICATEURS POSSIBLES

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la Loi sur l'accès à l'information ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la Loi sur la preuve au Canada. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



RCMP·GRC



ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA



BULLETIN DE L'ÉQUIPE NATIONALE DES INFRASTRUCTURES ESSENTIELLES

SENSIBILISATION DES AGENTS

Indices d'attentats potentiels dans des zones d'affluence 2016-03-22

À l'appui de la stratégie adoptée par le gouvernement du Canada pour assurer la résilience des infrastructures essentielles (IE), la Gendarmerie royale du Canada (GRC) évalue et signale l'information relative aux menaces et à la criminalité dirigées contre les IE canadiennes. Ces renseignements ou ces éléments d'information peuvent servir à protéger les IE du Canada. L'information contenue dans le présent bulletin date du 22 mars 2016. Les membres des organismes d'application de la loi font partie du secteur de la Sécurité, que le gouvernement du Canada considère comme l'un des dix secteurs d'IE au Canada.

CONTEXTE

Le présent bulletin de sensibilisation des agents (BSA) est publié pour mettre en lumière les indices d'attentats possibles dans des lieux bondés (p. ex. des stations de transport en commun et des installations de divertissement) dans la foulée des attentats perpétrés à Bruxelles, en Belgique.

Trois explosions ont frappé Bruxelles le 22 mars 2016, faisant au moins 34 morts et 180 blessés.^{1 2} Deux détonations ont dévasté l'aire des départs de l'aéroport international de Zaventem et une autre explosion a frappé la station de métro Maelbeek. On a appris depuis qu'au moins une des deux explosions à l'aéroport était un attentat-suicide.³ Toujours à l'aéroport, la police a découvert une ceinture d'explosifs qui n'avait pas explosé ainsi qu'un AK-47.⁴ Ces attentats sont survenus quatre jours après la capture à Bruxelles de Salah ABDESLAM, le principal suspect dans les attentats terroristes de Paris du 13 novembre 2015.⁵

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la *Loi sur la preuve au Canada*. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



ÉVALUATION DE L'ENIE

Le 22 mars 2016, l'État islamique (EI) a revendiqué la responsabilité des attentats, selon une déclaration diffusée par l'agence Amaq, un site Web qui serait proche du groupe extrémiste. Le message précisait que la Belgique avait été ciblée en raison de sa participation à la coalition internationale qui lutte contre l'EI.⁷

L'ENIE ne dispose pour le moment d'aucun renseignement laissant craindre un attentat imminent contre des infrastructures essentielles (IE) canadiennes et

Les indicateurs comportementaux qui suivent peuvent trahir la préparation ou la perpétration imminente d'attentats dans des zones d'affluence. Il importe de se rappeler qu'il faut évaluer l'ensemble des indicateurs comportementaux et des circonstances avant d'entreprendre une intervention des forces de l'ordre.

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la *Loi sur la preuve au Canada*. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



RECOMMANDATIONS

Il importe que tous les partenaires, des organismes d'application de la loi et des services de sécurité du secteur privé, signalent ce qui leur semble suspect. Le personnel de première ligne est le mieux placé pour observer les comportements suspects. Il connaît le milieu dans lequel il évolue et reconnaît ce qui fait partie de la routine. Un incident seul peut sembler anodin, mais plusieurs incidents pris ensemble peuvent trahir une menace réelle.

L'ENIE encourage les lecteurs du présent document à signaler aux organismes locaux d'application de la loi toute activité suspecte ou criminelle. Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité qui pourrait menacer la sécurité nationale du Canada, communiquez avec :

Le Réseau info-sécurité nationale : 1-800-420-5805
Le Service canadien du renseignement de sécurité (SCRS) : 613-993-9620

Rédigé par : Équipe nationale des infrastructures essentielles
Opérations criminelles de la Police fédérale
Courriel : SIR-SIS@RCMP-GRC.GC.CA

MANIPULATION DE RENSEIGNEMENTS

Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la *Loi sur la preuve au Canada*. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



- ¹ (U) <http://www.cnn.com/2016/03/22/europe/brussels-explosions/index.html>
- ² (U) <http://www.theguardian.com/world/2016/mar/22/brussels-airport-explosions-heard>
- ³ (U) <http://www.theguardian.com/world/2016/mar/22/brussels-airport-explosions-heard>
- ⁴ (U) ESISC, 2016-03-22
- ⁵ (U) <http://www.bbc.com/news/world-europe-35869985>
- ⁶
- ⁷ (U) https://www.washingtonpost.com/world/brussels-on-high-alert-after-explosions-at-airport-and-metro-station/2016/03/22/b5e9f232-f018-11e5-a61f-e9c95c06edca_story.html?hpid=hp_hp-banner-main_brussels-635am-mobile%3Ahomepage%2Fstory
- ⁸ (U) <https://sm.asisonline.org/Pages/A-Threat-in-the-Crowd.aspx>
-

MANIPULATION DE RENSEIGNEMENTS

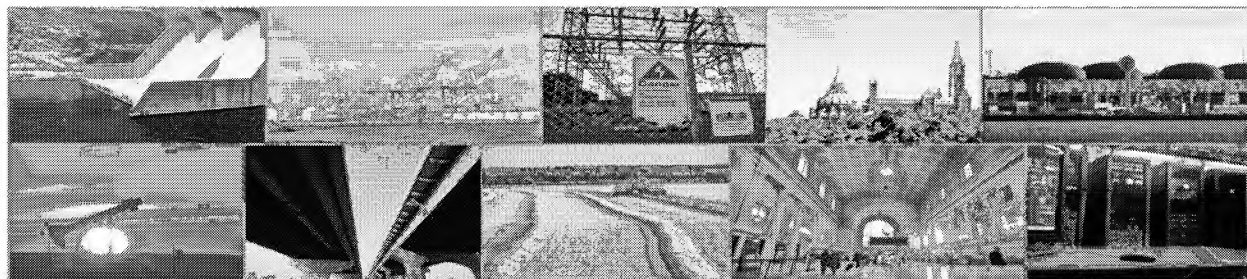
Le présent document appartient à la Gendarmerie royale du Canada (GRC). Son contenu est tiré de plusieurs sources dont l'information est en vigueur à la date de publication du document. Il est transmis à titre confidentiel à votre service ou organisme, qui peut le diffuser à des organismes d'application de la loi ou à des partenaires de l'application de la loi qui ont besoin de l'information (besoin de savoir). Ce document ne doit pas être réutilisé, en tout ou en partie, sans le consentement de l'auteur. Les commentaires relatifs au présent document doivent être envoyés par courriel au directeur général, Opérations criminelles de la Police fédérale (OCPF).

Le présent document peut faire l'objet d'une exception obligatoire en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*. Les renseignements qu'il contient peuvent également être protégés par les dispositions de la *Loi sur la preuve au Canada*. Ils ne peuvent pas être diffusés ou utilisés comme preuve sans que l'on ait consulté au préalable le directeur général, Opérations criminelles de la Police fédérale (OCPF).



RCMP-GRC

ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA



BULLETIN DE L'ÉQUIPE NATIONALE DES INFRASTRUCTURES ESSENTIELLES

SENSIBILISATION DES AGENTS :

Attentat à Orlando

Indices d'attentats potentiels dans des lieux de rassemblement 2016-06-14

À l'appui de la stratégie adoptée par le gouvernement du Canada pour assurer la résilience des infrastructures essentielles (IE), la Gendarmerie royale du Canada (GRC) évalue et signale l'information relative aux menaces et à la criminalité dirigées contre les IE canadiennes. Ces renseignements ou ces éléments d'information peuvent servir à protéger les IE du Canada. L'information contenue dans le présent bulletin date du 14 juin 2016. Les membres des organismes d'application de la loi font partie du secteur de la Sécurité, que le gouvernement du Canada considère comme l'un des 10 secteurs d'IE au Canada.

CONTEXTE

Le présent bulletin de sensibilisation des agents (BSA) paraît pour mettre en lumière les indices d'attentats possibles dans des lieux de rassemblement (p. ex. des événements sportifs, des stations de transport en commun et des installations de divertissement) dans la foulée de l'attentat perpétré le 12 juin 2016 à la boîte de nuit Pulse à Orlando (Floride).

Vers 2 h 02 le 12 juin 2016, un tireur solitaire a ouvert le feu à l'intérieur du Pulse, une boîte de nuit gaie populaire, blessant mortellement 49 personnes et en blessant 53 autres¹. L'agresseur, Omar MATEEN, âgé de 29 ans, a appelé le 911 au cours d'une confrontation de trois heures avec la police et a prêté allégeance à l'État islamique². Vers 5 h, les groupes tactiques d'intervention du Service de police d'Orlando (SPO) se sont introduits de force dans l'immeuble et ont abattu le tireur après que celui-ci ait fait feu sur eux. Tout semble indiquer qu'Omar MATEEN aurait été motivé par de la propagande extrémiste sur Internet. Par ailleurs, le FBI aurait effectué deux enquêtes antérieures sur les liens éventuels d'Omar MATEEN à l'extrémisme violent^{3 4}.

HANDLING INSTRUCTIONS

This document is the property of the Royal Canadian Mounted Police (RCMP). The document is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to law enforcement and law enforcement partners with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed by email to the Director General, Federal Policing Criminal Operations (FPCO).

This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Director General, Federal Policing Criminal Operations (FPCO).



L'attentat à Orlando est représentatif d'une tendance préoccupante d'attaques s'inspirant de l'extrémisme violent dans des lieux de rassemblement qui permettent aux agresseurs de faire le plus de victimes possible. Le 22 mars 2016, trois explosions ont frappé Bruxelles, faisant 35 morts (32 victimes et trois agresseurs) et au moins 180 blessés^{5 6} : deux déflagrations ont dévasté l'aire de départ de l'aéroport international de Zaventem et une troisième explosion a ravagé la station de métro Maelbeek^{7 8}. L'EI a revendiqué la responsabilité des attentats et a déclaré que la Belgique était ciblée à cause de sa participation à la coalition internationale luttant contre eux⁹. Le 13 novembre 2015, des attentats quasi simultanés en France ont ciblé un stade de soccer, de multiples restaurants et une salle de concert à Paris. Les fusillades et les déflagrations ont fait 130 morts et des centaines de blessés. L'EI a aussi revendiqué la responsabilité de ces attaques, déclarant qu'elles constituaient des représailles aux frappes aériennes de la France contre des cibles de l'EI en Syrie et en Irak.

Le 5 décembre 2015, 14 personnes ont été tuées et 22 gravement blessées lors d'une fusillade et une tentative d'attentat à la bombe à San Bernardino (Californie). Les agresseurs, qui s'étaient apparemment autoradicalisés après avoir été exposés à la propagande de l'EI, ont ciblé une session de formation et une réception des Fêtes du département de la santé publique du comté de San Bernardino (réunissant quelque 80 employés)¹⁰.

ÉVALUATION DE L'ENIE

L'attentat à Orlando est la tuerie la plus meurtrière de l'histoire des États-Unis et

À quelques semaines seulement de l'attentat, le porte-parole officiel de l'EI, Abou Mohammed al-Adnani a diffusé un message enregistré exhortant les partisans à lancer des attaques contre les États-Unis et l'Europe durant le ramadan.

Si les motifs précis de l'attentat à Orlando font toujours l'objet d'une enquête, l'attaque constitue un autre exemple de la façon dont les extrémistes locaux et les acteurs solitaires sont en mesure d'exécuter des attentats rigoureusement planifiés, sans le soutien direct d'une organisation terroriste. Il faut aussi reconnaître le risque que la récente exhortation d'AL-ADNANI à exécuter des attaques contre des civils durant le ramadan inspire des incidents similaires.

En plus d'être considéré comme un cas d'extrémisme local, l'attentat à Orlando est également catégorisé comme crime haineux contre la communauté LGBT. La première édition du Mois de la fierté au Canada, qui vise à célébrer la diversité fondée sur le sexe et l'orientation sexuelle, a débuté le 1er juin dernier et prévoit un éventail d'activité et d'événements (dont des défilés) à l'échelle du pays.

L'ENIE ne dispose pour le moment d'aucun renseignement laissant craindre un attentat imminent et

. Toutefois, certains jugent que les attentats

HANDLING INSTRUCTIONS

This document is the property of the Royal Canadian Mounted Police (RCMP). The document is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to law enforcement and law enforcement partners with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed by email to the Director General, Federal Policing Criminal Operations (FPCO).

This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Director General, Federal Policing Criminal Operations (FPCO).

de Paris et de Bruxelles, dont l'EI a revendiqué la responsabilité, auraient été perpétrés en représailles contre la participation de la France et de la Belgique à la coalition contre l'EI.

Les indicateurs comportementaux qui suivent peuvent trahir la préparation ou la perpétration imminente d'attentats dans des lieux de rassemblement Il importe de se rappeler qu'il faut évaluer l'ensemble des indicateurs comportementaux et des circonstances avant d'entreprendre une intervention des forces de l'ordre.

HANDLING INSTRUCTIONS

This document is the property of the Royal Canadian Mounted Police (RCMP). The document is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to law enforcement and law enforcement partners with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed by email to the Director General, Federal Policing Criminal Operations (FPCO).

This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Director General, Federal Policing Criminal Operations (FPCO).



RECOMMANDATIONS

Il est important que tous les partenaires, y compris les organismes d'application de la loi et le personnel de sécurité du secteur privé, signalent tout ce qui leur semble suspect. Le personnel de première ligne est le mieux placé pour observer les comportements suspects. Il connaît le milieu dans lequel il évolue et reconnaît ce qui fait partie de la routine. Un incident particulier peut sembler insignifiant, mais s'il fait suite à plusieurs autres incidents documentés, il pourrait signaler une menace sérieuse.

L'ENIE encourage les destinataires du présent document à signaler à leur service de police local toute activité suspecte ou criminelle. Pour signaler une activité suspecte, un cas d'extrémisme criminel ou toute autre activité qui pourrait menacer la sécurité nationale du Canada, communiquez avec :

Réseau info-sécurité nationale : 1-800-420-5805
Service canadien du renseignement de sécurité (SCRS) : 613-993-9620

Rédigé par : Équipe nationale des infrastructures essentielles
Opérations criminelles de la Police fédérale
Courriel : SIR-SIS@RCMP-GRC.GC.CA

¹ (NC) <http://www.orlandosentinel.com/news/pulse-orlando-nightclub-shooting/os-orlando-nightclub-omar-mateen-profile-20160613-story.html>

² (NC) https://www.washingtonpost.com/news/post-nation/wp/2016/06/13/police-orlando-gunman-was-cool-and-calm-during-hostage-standoff/?utm_term=.a66c125d31d4

³ (NC) https://www.washingtonpost.com/news/post-nation/wp/2016/06/13/police-orlando-gunman-was-cool-and-calm-during-hostage-standoff/?utm_term=.6d67f78d3a01

⁴ (NC) The Soufan Group. The Orlando Attack : Assessing Threats to Soft Targets, 2016-06-13

⁵ (NC) <http://www.cnn.com/2016/03/22/europe/brussels-explosions/index.html>

⁶ (NC) <http://www.theguardian.com/world/2016/mar/22/brussels-airport-explosions-heard>

⁷ (NC) <http://www.theguardian.com/world/2016/mar/22/brussels-airport-explosions-heard>

⁸ (NC) ESISC, 2016-03-22

⁹ (NC) https://www.washingtonpost.com/world/brussels-on-high-alert-after-explosions-at-airport-and-metro-station/2016/03/22/b5e9f232-f018-11e5-a61f-e9c95c06edca_story.html?hpid=hp_hp-banner-main_brussels-635am-mobile%3Ahomepage%2Fstory

¹⁰ <http://www.pe.com/articles/similarities-805586-orlando-san.html>

¹² (NC) The Soufan Group. The Orlando Attack : Assessing Threats to Soft Targets, 2016-06-13

¹³ (NC) <https://sm.asisonline.org/Pages/A-Threat-in-the-Crowd.aspx>

HANDLING INSTRUCTIONS

This document is the property of the Royal Canadian Mounted Police (RCMP). The document is derived from various sources with information effective as of the date of publication. It is provided to your agency/department in confidence and may be further disseminated by your agency/department to law enforcement and law enforcement partners with the need to know. It must not be reused in any way, in whole or in part, without the consent of the originator. Any feedback should be directed by email to the Director General, Federal Policing Criminal Operations (FPCO).

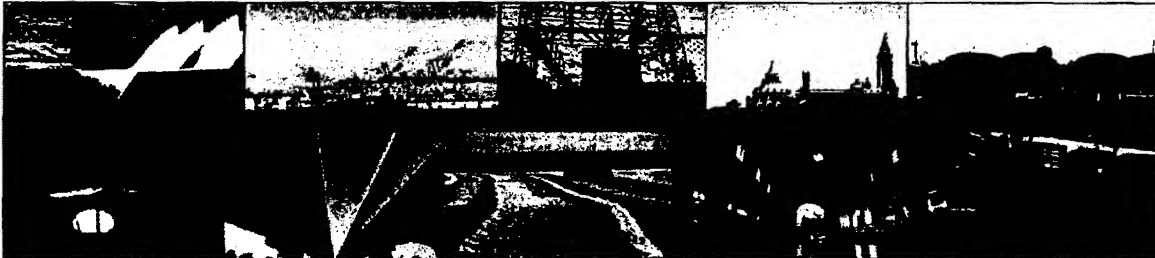
This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Director General, Federal Policing Criminal Operations (FPCO).

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

RCMP-GRC



ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA



NATIONAL CRITICAL INFRASTRUCTURE BULLETIN

UPDATE: EXTREMIST INSIDERS IN THE AVIATION INDUSTRY

2016-02-10

The RCMP, in support of the Government of Canada's (GoC) strategy to ensure critical infrastructure (CI) resiliency, assesses, evaluates and reports on information regarding threats and criminality to Canada's CI. This intelligence and/or information may be used to assist in the protection of Canada's CI. Information contained within this Assessment is current as of **February 10, 2016. This document is deemed to be most applicable to airport policing units, other first responder and law enforcement units based at airports, and airport/airline security personnel.**

KEY FINDINGS

- the global nature of the aviation industry, coupled with the general threat environment, requires law enforcement and security personnel to be aware of the tradecraft and trends inherent in known international cases involving aviation insiders.

Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

BACKGROUND & LIMITATIONS

In 2013, NCIT issued an assessment that examined trends and tradecraft related to known cases of extremism found within the aviation industry.

(Please refer to APPENDICES A and B for an illustrative guide case summaries.)

ASSESSMENT

- the global nature of the aviation industry, coupled with the general threat environment, requires law enforcement and security personnel to be aware of the tradecraft and trends inherent in known international cases involving aviation insiders.

- Historically, confirmed extremist plots involving airport or airline employees have had extremely limited success. The low success rate can be attributed to the detection and disruption of most plots by authorities.¹

Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.



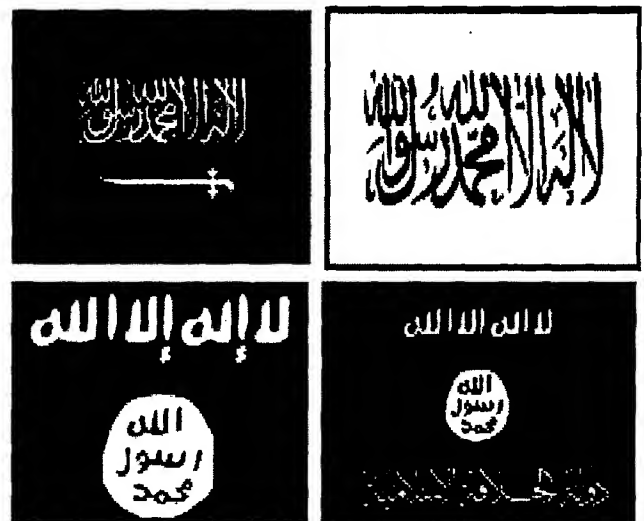
Royal Canadian Gendarmerie royale
NOT REVIEWED

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

insiders as a successful tactic worth adopting or repeating in the future. This possibility makes the detection and reporting of suspicious behaviours increasingly vital.

BEHAVIOURAL INDICATORS

ii) Potential cases of radicalization



Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.

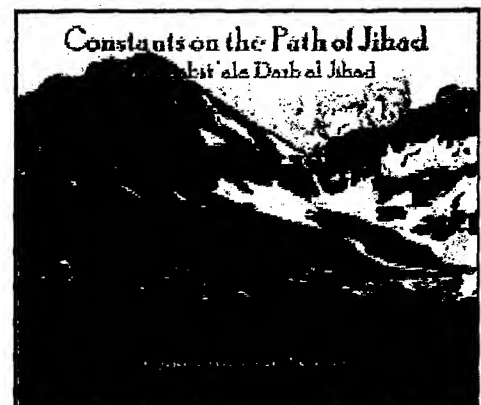
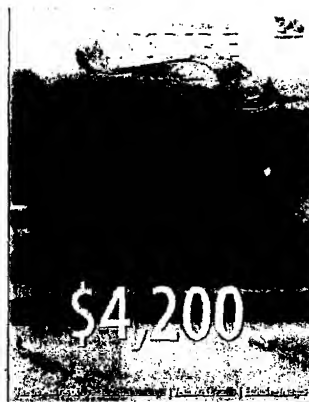


Royal Canadian Gendarmerie royale
NOT REVIEWED

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY



AL HAYAT



Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

POTENTIAL MITIGATIVE ACTIONS



Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.



Royal Canadian Gendarmerie royale
NOT REVIEWED

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

RECOMMENDATIONS

NCIT encourages recipients of this document to report information concerning suspicious or criminal activity to local law enforcement organizations. To report information regarding suspicious activity, criminal extremism, or other activities which could pose a threat to Canada's national security call:

**National Security Information Network at 1-800-420-5805
Canadian Security Intelligence Service (CSIS) at (613)-993-9620**

**Prepared by: National Critical Infrastructure Team
Federal Policing Criminal Operations
Email: SIR-SIS@RCMP-GRC.GC.CA**

Federal Policing Criminal Operations

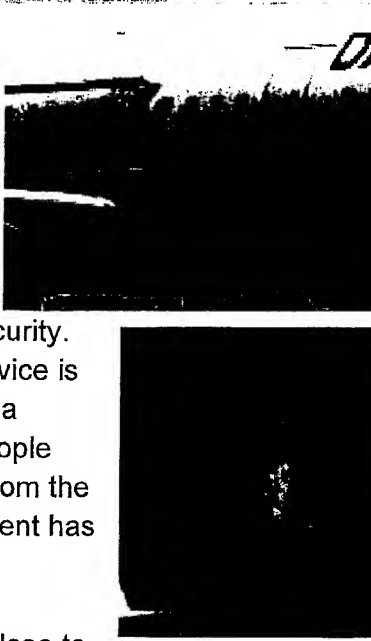
This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.



Royal Canadian Gendarmerie royale
NOT REVIEWED

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

APPENDIX B ~ SUMMARIES OF CONFIRMED AND SUSPECTED CASES OF EXTREMISM WITHIN THE AVIATION INDUSTRY

- On 2016-02-16, Daallo Airlines Flight 159 departed from Aden Adde International Airport in Mogadishu, Somalia. According to reports, a suspected suicide bomber boarded the aircraft and detonated an explosive 15 minutes after takeoff that blew a hole through the fuselage. CCTV footage taken at the airport prior to the flight allegedly shows two men handing what appears to be a laptop computer to the suspected bomber after the suspect passed through security. At least one of the men who delivered the laptop-like device is believed to be an airport employee and is seen wearing a bright orange, high-visibility security vest. At least 20 people were arrested in connection with the explosion. Aside from the bomber, all on board survived what the Somali government has confirmed to be a coordinated act of terrorism.
 
- According to a mainstream media outlet citing sources close to the Egyptian investigation into the October 2015 downing of MetroJet Flight 9268, four individuals have been detained in connection with the crash. The plane crashed in the Sinai Peninsula after taking off from Sharm el-Sheikh International Airport, killing all 224 people aboard. Several experts have confirmed an explosive device was responsible. Shortly after the crash, the Islamic State in Iraq and Syria (ISIS) claimed responsibility. An EgyptAir mechanic whose cousin reportedly joined ISIS is suspected of placing the device on board the flight. The sources said the mechanic had been detained along with a baggage handler suspected of helping him put the device on board. Two airport policemen have also been detained.
- Terry Loewen**, 58, worked as an avionics technician at Kansas's Wichita Mid-Continent Airport until he was arrested in 2013 for allegedly planning to detonate a vehicle-borne improvised explosive device (VBIED) on the airport's tarmac, in proximity to passenger planes and terminals. By using his employee access card to enter the tarmac on an early December morning, he believed he would inflict maximum physical and economic damage by executing the attack just prior to the Christmas holiday, on one of the busiest travel days of the year. According to court documents, Loewen undertook the following activities: studying the layout of the

Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.



Royal Canadian Gendarmerie royale
NOT REVIEWED

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

airport and taking photographs of access points; researching flight schedules; assisting in acquiring components for the explosive device; and talking about his commitment to trigger the device and martyr himself. Loewen was sentenced to 20 years in prison.

- **Belal Sadallah Khazaal** worked at Qantas as a baggage handler for 12 years (1988- 2000). During this time, he became known to Australian authorities. According to a CIA report, Khazaal was said to have trained in a military camp in Afghanistan in 1998 and to have become a confidant of Al Qaeda leaders. Khazaal was found to have produced a 110-page manual that included instruction on bomb-making, assassinations, kidnappings, and shooting down planes. A court ruling found the manual intended to help facilitate terrorist acts. In 2009, Khazaal was sentenced to 12 years in prison.
- **Rajib Karim** worked as a software developer for British Airways (BA) from 2007 until his arrest in 2010. During his trial, prosecutors alleged Karim deliberately found work with BA to advise terrorists in Yemen, Pakistan, and Bangladesh on details concerning airport security scanners, allowable liquids, and immigration questions asked of travelers. During his time at BA, Karim was in email communication with Anwar Al-Awlaki, who was then a senior member of Al Qaeda in the Arabian Peninsula. Al-Awlaki instructed Karim to recruit co-workers who might know how to circumvent airport x-ray machines. In response, Karim was in contact with a baggage handler and an associate in airport security at Heathrow Airport. Karim also offered to take advantage of a possible labor strike by BA personnel by applying for a temporary cabin-crew position. In 2011, Karim was sentenced to 30 years in prison.
- **Samina Malik** worked as a shop assistant on the air-side of Heathrow Airport. In 2006, Malik was in e-mail communication with convicted extremist Sohail Qureshi. The latter admitted to planning an overseas terrorist attack, possibly against British troops in Afghanistan. According to police, Malik "provided Qureshi with the latest security measures in place" at the

From: "Khan Inqlabi" <@hotmail.com>
To: @hotmail.co.uk
Subject: salams
Date: Sun, 08 Oct 2006 11:12:54 +1400

Salams...

Sis, I hope u get this email before anyone else does...

Wat is the situation like at work? Is the checking still very harsh? or have things cooled down a bit?

bara'Allah feek...

ws wr wb

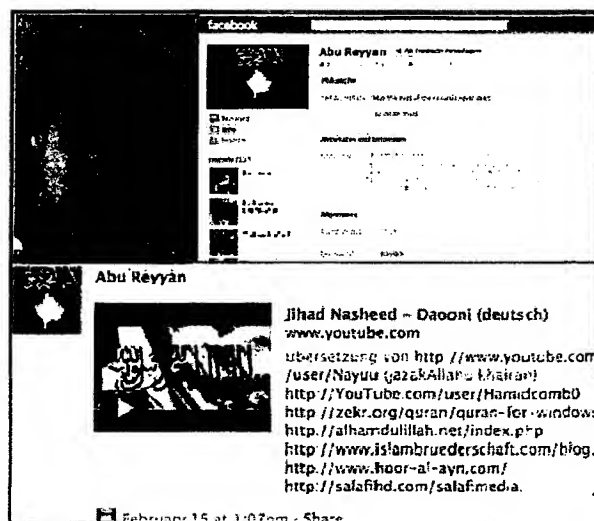
Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

airport. Qureshi apparently wished to slip out of the U.K. unnoticed to carry out the overseas operation. Before his attempted departure, Qureshi wrote to Malik: "Sis I hop u get this email before anyone else does. What is the system like at work? Is the checking still very harsh? Or have things calmed down a bit? ... Delete after read!" In Malik's reply, she detailed the security measures, including regimes around pat-down searches and checks on liquids. She signed off with the line, "A stranger awaiting martyrdom." Among the items found in Qureshi's luggage: an AQ training manual, night-vision goggles, and Canadian and U.S. military manuals which referred to guerilla tactics and urban warfare.

- **Asmin Amin Tariq** was one of 24 people originally arrested in conjunction with the 2006 liquid explosives plot against 10 trans-Atlantic flights. Prior to his arrest, Tariq worked as a security guard for Jet Airways at Heathrow Airport. As such, he had 24-hour access to all areas of the airport. According to the U.S. Transportation Security Administration, Tariq helped Islamic extremists pose as airport employees so they could conduct surveillance of security procedures at Heathrow. In addition, Tariq allegedly provided information about airport security procedures to the would-be bombers.
- **Arid Uka** worked in the mail room at Frankfurt Airport's Terminal 2. On 2011-03-02, he walked outside of the terminal and approached a bus. After confirming that the bus carried U.S. personnel bound for Afghanistan, he boarded it and fired nine shots with a pistol, killing the bus driver and one soldier. Two other soldiers were injured. According to open sources, one of the main triggers for Uka's actions was an online video-clip of a fictitious rape scene where the perpetrators were U.S. military personnel. In 2012, Uka was sentenced to life in prison.
- **Gregory Patterson**, a Muslim convert, worked in a duty-free shop at Los Angeles International Airport (LAX) in 2005. He was one of four operatives recruited to a California-based extremist group, Jami'iyat al-Islam Saheeh (JIS), who considered attacking the airport's El Al Airlines ticket counter. Plot mastermind Kevin James'



Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.

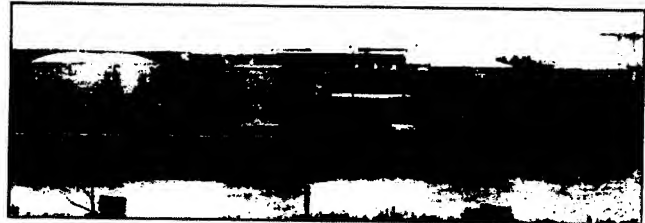


Royal Canadian Mounted Police
NOT REVIEWED

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

plea agreement states that "in March 2005, the defendant wrote a letter to [co-conspirator Levar] Washington telling him that Patterson should keep his job at [the airport]". Patterson conducted surveillance and Internet research on El Al. He also purchased a rifle and conducted target practice, and learned how to make homemade explosives. He was sentenced to 12.5 years in prison.

- **Russell Defreitas** worked as a cargo handler at JFK International Airport and then as a trainee supervisor for a cargo company until he was laid off in 2001. Defreitas was the mastermind behind the 2007 plot against JFK's jet fuel storage facilities and pipeline systems. According to taped conversations and an FBI informant, Defreitas said his "unique knowledge" of the airport and its vulnerabilities would be of utmost utility for advancing the attack. According to court documents, he told co-conspirators that he had tested the security apparatus multiple times when stealing cargo. Defreitas is alleged to have taken photo/video footage of the airport to help identify targets; acquired Google Earth images of the target area; studied airport security; and planned escape routes. In 2011, he was sentenced to life in prison.



- **Adem Yilmaz** worked as a security guard for rail operator Deutsche Bahn at Frankfurt Airport Regional railway station from 1997 to 2002. This station is located underneath Frankfurt Airport's Terminal 1. A member of Islamic Jihad Union, Yilmaz was part of a four-person cell that had originally considered targeting Frankfurt Airport. Over time, the targets of the explosives plot changed to other German-based targets, including American ex-patriots and the US Air Force's Ramstein Air Base. In 2010, Yilmaz was sentenced to 11 years in prison.
- **Muhammad Syahrir** worked for Indonesia's national airline, Garuda, as an aircraft technician. Police believe he infiltrated Garuda as part of a wider plot against the country's airline sector. A member of AQ-affiliated Jamaah Islamiyah, Syahrir was also believed to be a skilled bomb maker associated with the bombing of Indonesian hotels in 2009. He was killed in a police raid.

Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.

PROTECTED A //THIRD-PARTY RULE// CANADIAN EYES ONLY

ENDNOTES

¹ "EXTREMIST INSIDERS IN THE AVIATION INDUSTRY: TRENDS AND TRADecraft", NCIT, RCMP, 2013-05-01.

Federal Policing Criminal Operations

This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the OIC National Security Criminal Operations, RCMP.



Royal Canadian Gendarmerie royale
NOT REVIEWED

Canada

A0000355_38-000038

A0326651_14-000154